Symantec AntiVirus™ Corporate Edition Installation Guide

Symantec AntiVirus™ Corporate Edition Installation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.
Documentation version 9.0
PN: 10223892

Copyright Notice

Trademarks

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/ function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT
Symantec AntiVirus

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use the number of copies of the Software as have been licensed to You by Symantec under a License Module. If the Software is part of a suite containing multiple Software titles, the number of copies You may use may not exceed the aggregate number of copies indicated in the License Module, as calculated by any combination of licensed Software titles. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;
B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;
D. use the Software in accordance with any written agreement between You and Symantec; and
E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

You may not:

A. copy the printed documentation that accompanies the Software;
B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
D. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
E. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;
F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor
G. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. Licensee agrees to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

8. Additional Uses and Restrictions:

A. If the Software You have licensed is a specified Symantec AntiVirus™ for a third party product or platform, You may only use that specified Software with the corresponding product or platform. You may not allow any computer to access the Software other than a computer using the specified product or platform. In the event that You wish to use the Software with a certain product or platform for which there is no specified Software, You may use Symantec AntiVirus Scan Engine.

B. If the Software you have licensed is Symantec AntiVirus utilizing Web Server optional licensing as set forth in the License Module, the following additional use(s) and restriction(s) apply:

i) You may use the Software only with files that are received from third parties through a web server;

ii) You may use the Software only with files received from less than 10,000 unique third parties per month; and

iii) You may not charge or assess a fee for use of the Software for Your internal business.

C. If the Software You have licensed is Symantec AntiVirus Corporate Edition, You may not use the Software on or with devices on Your network running embedded operating systems specifically supporting network attached storage functionality without separately licensing a version of such Software specifically licensed for a specific type of network attached storage device under a License Module.

D. If the Software You have licensed is Symantec AntiVirus for EMC® Celerra™ File Server, You may use the Software only with EMC Celerra servers and only if You have a license to the Software for each Celerra AntiVirus Agent (CAVA) associated with each such server. You may not allow any computer to access the Software other than an EMC Celerra server.

E. If the Software You have licensed is Symantec Client Security, this Software utilizes the Standard Template Library, a C++ library of container classes, algorithms, and iterators. Copyright © 1996-1999. Silicon Graphics Computer Systems, Inc. Copyright © 1994. Hewlett-Packard Company.

EMC and Celerra are trademarks or registered trademarks of EMC Corporation in the U.S. and other countries.

Sun Microsystems, Inc. Binary Code License Agreement

READ THE TERMS OF THIS AGREEMENT AND ANY PROVIDED SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT") CAREFULLY BEFORE OPENING THE SOFTWARE MEDIA PACKAGE. BY OPENING THE SOFTWARE MEDIA PACKAGE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCESSING THE SOFTWARE ELECTRONICALLY, INDICATE YOUR ACCEPTANCE OF THESE TERMS BY SELECTING THE "ACCEPT" BUTTON AT THE END OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL THESE TERMS, PROMPTLY RETURN THE UNUSED SOFTWARE TO YOUR PLACE OF PURCHASE FOR A REFUND OR, IF THE SOFTWARE IS ACCESSED ELECTRONICALLY, SELECT THE "DECLINE" BUTTON AT THE END OF THIS AGREEMENT.

1. LICENSE TO USE.

Sun grants you a non-exclusive and non-transferable license for the internal use only of the accompanying software and documentation and any error corrections provided by Sun (collectively "Software"), by the number of users and the class of computer hardware for which the corresponding fee has been paid.

2. RESTRICTIONS.

Software is confidential and Copyright 1994-2004 Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement.

3. LIMITED WARRANTY.

Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software.

4. DISCLAIMER OF WARRANTY.

UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

5. LIMITATION OF LIABILITY.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose.

6. Termination.

This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Upon Termination, you must destroy all copies of Software.

7. Export Regulations.

All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

8. U.S. Government Restricted Rights.

If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

9. Governing Law.

Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

10. Severability.

If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

11. Integration.

This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

JAVA^{TM} 2 RUNTIME ENVIRONMENT (J2RE), STANDARD EDITION, VERSION 1.4.1_X SUPPLEMENTAL LICENSE TERMS

These supplemental license terms (“Supplemental Terms”) add to or modify the terms of the Binary Code License Agreement (collectively, the “Agreement”). Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

1. Software Internal Use and Development License Grant.

Subject to the terms and conditions of this Agreement, including, but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the binary form of the Software complete and unmodified for the sole purpose of designing, developing, testing, and running your Java applets and applications intended to run on Java-enabled general purpose desktop computers and servers (“Programs”).

2. License to Distribute Software.

Subject to the terms and conditions of this Agreement, including, but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified (unless otherwise specified in the applicable README file) and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. (vi) include the following statement as part of product documentation (whether hard copy or electronic), as a part of a Copyright 1994-2004 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.

(LFI#133025/Form ID#011801)

Contents

Technical support

Chapter 1 Introducing Symantec AntiVirus

Chapter 2 Planning the installation

Chapter 3 Preparing to install Symantec AntiVirus

Chapter 4 Migrating to the current version of Symantec AntiVirus

Chapter 7 Installing Symantec AntiVirus clients

Appendix A Windows Installer (.msi) command-line reference

Index

Chapter 1

Introducing Symantec AntiVirus

This chapter includes the following topics:

About Symantec AntiVirus

Symantec AntiVirus Corporate Edition (Symantec AntiVirus) provides scalable, cross-platform antivirus protection for workstations and network servers throughout the enterprise. Using the enhanced security features and centralized policy management of Symantec AntiVirus, administrators can manage clients and servers assigned to logical groups. In addition, administrators can create, deploy, and lock down security policies and settings to keep systems up-to-date and properly configured at all times. The central management console enables administrators to audit the network, identify unprotected nodes, and apply the appropriate security protection before a threat occurs.

Symantec AntiVirus lets you do the following:

- Manage the deployment, configuration, updating, and reporting of antivirus protection from an integrated management console.

- Quickly respond to virus outbreaks and deploy updated virus definitions.
- Provide a high level of protection and an integrated response to security threats for all users that connect to your network, including telecommuters with always-on connections and mobile users with intermittent connections to your network.
- Obtain a consolidated view of multiple security components across all of the workstations on your network.
- Perform a customizable, integrated installation of all of the security components and set policies simultaneously.

Components of Symantec AntiVirus

Table 1-1 lists and describes the main components of Symantec AntiVirus.

You can also view supported operating systems for each feature.

See "Installation requirements" on page 69.

Table 1-1 Components of Symantec AntiVirus

Component	Description
The Symantec System Center	Performs management operations such as the following: ■ Installing antivirus protection on workstations and network servers. ■ Updating virus definitions. ■ Managing network servers and workstations running Symantec AntiVirus.
Symantec AntiVirus server	■ Protects the supported Windows and NetWare computers. ■ Pushes configuration and virus definitions files updates to managed clients.
Symantec AntiVirus client	Provides antivirus protection for networked and non-networked computers. Symantec AntiVirus protects supported Windows computers.
LiveUpdate	Provides the capability for computers to automatically pull updates of virus definitions files from the Symantec LiveUpdate server or an internal LiveUpdate server.

Table 1-1 Components of Symantec AntiVirus

Component	Description
Central Quarantine	Works as part of the Digital Immune System to provide automated responses to heuristically detected new or unrecognized viruses and does the following: ■ Receives unrepaired infected items from Symantec AntiVirus servers and clients. ■ Forwards suspicious files to Symantec Security Response. ■ Returns updated virus definitions to the submitting computer. **Note:** Symantec Security Response was formerly known as Symantec AntiVirus Research Center.

What's new in this release

Symantec AntiVirus includes new features, as well as improvements to existing features. Table 1-2 lists and describes what's new in this release.

Table 1-2 New features in Symantec AntiVirus

Feature	Description
Windows Installer (.msi) technology-based client and server installations	Lets you install Symantec AntiVirus clients and servers using Windows Installer technology to support .msi-based installation and deployment. The benefits of using Windows Installer technology include the following: ■ Provides fully configurable installations using the standard Microsoft Windows Installer options that can be used in conjunction with Symantec AntiVirus-specific features ■ Reduces installation and deployment file size ■ Supports the installation of in-field patches for security updates and upgrades ■ Supports additional .msi-supported third-party deployment tools such Active Directory and Tivoli
Deployment of installations without granting administrator rights on the target computer	Lets you install Symantec AntiVirus from the Microsoft Management Console (MMC) using Elevated Privileges, rather than granting administrative privileges to the user on the target computer.

Table 1-2 New features in Symantec AntiVirus

Feature	Description
Auto-Protect	Replaces and scans faster than Realtime File Protection. Auto-Protect can be loaded on system startup, and then unloaded on system shutdown to help protect against viruses, such as Fun Love. It can be stopped and then reloaded immediately or when the computer restarts. Auto-Protect includes the following capabilities and features: ■ Scanning for Internet email protects both incoming and outgoing messages that use the POP3 or SMTP communications protocol. ■ SmartScan replaces Scan selected types and Scan selected exclusions options. SmartScan scans .exe and .doc files even if the file extensions for the .exe or .doc files are changed to extensions that it is not configured to scan. ■ File caching, which stores an index of clean files, can help track problems and fine tune Auto-Protect's memory usage. ■ Rtvscan, the main Symantec AntiVirus service, and Auto-Protect are separate components in the Windows version. If Rtvscan stops, Auto-Protect continues to detect viruses.
In-memory threat scanning	Lets you scan running processes to identify and handle threats that are loaded into memory.
Threat Tracer	Lets you identify the source of network share-based virus infections on computers that are running Windows NT-based operating systems. Threats can be traced using the source computer IP address and its NetBIOS name.
Expanded threat detection	Scans for new threats in the following categories: Spyware, Adware, Dialers, Joke Programs, Remote Access programs, Hack Tools, and Trackware. Other threats that do not meet these category requirements are included in the Security Risks category.
Moving clients between servers	Lets you move clients from one parent server to another using a drag-and-drop operation.

Table 1-2 New features in Symantec AntiVirus

Feature	Description
Forced LiveUpdate for Symantec AntiVirus clients	Provides a way to update virus definitions files when clients on which LiveUpdate is installed are using outdated files. When an update operation that ran at the server group level succeeds on all but a few clients, you can update the remaining clients immediately, even if they normally update using the Virus Definition Transport Method.
Symantec VPN Sentry	Prevents users with nonsecure computers from connecting to the corporate network through a VPN connection and ensures that a computer that is attempting to connect is compliant with the corporate security policy. You can allow or deny network access and remediate noncompliant clients.
Log forwarding	Lets you select the events that clients forward to their parent servers and that secondary servers forward to primary servers.
POP3 and SMTP Internet email scanning	Lets you configure Symantec AntiVirus clients to scan email body text and attachments that are transported using the POP3 or SMTP protocols. The ports that are scanned for POP3 and SMTP traffic are fully configurable.
Outbound email heuristics scanning	Helps you identify threats that may be contained in outgoing email messages using Bloodhound Virus Detection heuristics. Scanning outgoing email messages helps to prevent the spread of threats such as worms that can use email clients to replicate and distribute themselves across a network.
New platform support	The following platforms are now supported: ■ Windows XP Tablet PC (Symantec AntiVirus client) ■ Novell NetWare 6.5 (Symantec AntiVirus server)
New folder names	Folders that were named Symantec AntiVirus Corporate Edition, Norton AntiVirus Corporate Edition, or NAV in earlier product versions are now named Symantec AntiVirus.

How Symantec AntiVirus works

Symantec AntiVirus lets you deploy and manage security protection according to the requirements of your enterprise. To understand how Symantec AntiVirus works and to determine how you can most effectively implement a security solution, it is important to understand the following key concepts:

- The Symantec System Center
- Installation
- Protection updating
- Communication
- Alerting
- The Digital Immune System

How the Symantec System Center works

The Symantec System Center comprises components that let you perform management operations such as installing protection on workstations and network servers, updating virus definitions, and managing network servers and workstations running Symantec AntiVirus. The Symantec System Center also includes alerting capabilities.

The Symantec System Center is comprised of the following management components:

- The Symantec System Center console
- Alert Management System^2 (AMS^2) console
- Symantec AntiVirus snap-in
- Symantec Client Firewall snap-in
- NT Client Install tool
- AV Server Rollout Tool

Symantec System Center console

The Symantec System Center console lets you view and administer your Symantec AntiVirus network. The Symantec System Center console is installed to the computers from which you plan to manage your Symantec products. You must have at least one installation of the Symantec System Center console. If your organization is large or you work out of several offices, you can install the Symantec System Center to multiple computers by rerunning the installation program and selecting the appropriate option.

The Symantec System Center console is a Microsoft Management Console (MMC) snap-in. MMC is a common framework with no management functionality of its own. MMC serves as a central host from which you can run multiple network and component management applications, such as the Symantec System Center.

MMC must be installed on a local drive of a Windows NT 4.0 (Workstation or Server) computer. MMC installs automatically with supported Windows 2000 platforms. When the Symantec System Center is installed on this same computer, it snaps in to MMC.

Alert Management System console

The AMS^2 console is installed to the same computer on which the Symantec System Center console is installed and supports alerts from AMS^2 clients and servers. The AMS^2 console lets you configure alert actions for Symantec AntiVirus servers that have the AMS^2 service installed.

Symantec AntiVirus snap-in

The Symantec AntiVirus snap-in lets you perform management tasks from the Symantec System Center, including setup and configuration of client and server groups, event management, and protection updating.

Symantec Client Firewall snap-in

The Symantec Client Firewall snap-in lets you centrally distribute firewall policy files.

This snap-in is used for client firewall administration, which is not included with Symantec AntiVirus.

NT Client Install tool

The NT Client Install tool lets you remotely install the Symantec AntiVirus client to one or more Windows NT-based computers.

AV Server Rollout tool

The AV Server Rollout tool lets you remotely install the Symantec AntiVirus server to the Windows NT-based servers that you select.

How installation works

The methods that you use to install Symantec AntiVirus and the components that you select depend on how you plan to implement security at your site. Installation typically involves the following processes:

- Installing the Symantec System Center console and the default management components
- Installing Symantec AntiVirus servers
- Installing Symantec AntiVirus clients
- Installing the Central Quarantine Server and Console (optional)
- Installing and configuring the LiveUpdate Administration Utility (optional)

How protection updating works

Symantec AntiVirus provides the following methods for updating virus definitions files:

- Virus Definition Transport Method

  This method is a push operation that starts when a primary server on your network receives new virus definitions from the Symantec LiveUpdate server or, if you have one, an internal LiveUpdate server. The definitions are then pushed to secondary servers and from the secondary servers to the clients that they manage.
- LiveUpdate

  This method is a pull operation that starts when a Symantec AntiVirus client or server uses LiveUpdate to request new virus definitions. LiveUpdate may be initiated manually or automatically according to a predefined schedule. The request may be directed to an internal LiveUpdate server, if you have one, or to the Symantec LiveUpdate server.

  LiveUpdate is the only method for updating virus definitions files that is supported on 64-bit computers.
- Central Quarantine polling

  This method is available if you have a Central Quarantine Server. You can configure the Central Quarantine Server to poll the Symantec LiveUpdate server for virus definitions files updates and then automatically push the new virus definitions to computers on the network.
- Intelligent Updater

  This method provides a self-extracting executable file that contains virus definitions files. These files are available for download from the Symantec Web site.

How Symantec AntiVirus communication works

Symantec AntiVirus employs the following forms of communication:

- Communication during Discovery
- Symantec AntiVirus server-to-client communication

Communication during Discovery

The Discovery Service allows the Symantec System Center to obtain information about the computers on the network that are running Symantec AntiVirus server.

When you perform a Discovery from the Symantec System Center console, the console broadcasts a message across the network. Symantec AntiVirus servers listen for and receive these messages, and return data (such as a server's address and server group) to the console. After the servers respond, the Symantec System Center can query each server for additional information, such as which computers running Symantec AntiVirus client report to the server. The Symantec System Center uses the data that it gathers from Discovery to display the system hierarchy in the console. Each server group is represented based on its server group membership.

Symantec AntiVirus server-to-client communication

Symantec AntiVirus servers communicate with the clients that they control to keep virus definitions files current, initiate client-side activities such as threat scans, and provide configuration information. Symantec AntiVirus clients communicate with their parent servers to provide status information and log data.

Communication for virus definitions updates

Communication occurs during the process of updating virus definitions files.

When you use the Virus Definition Transport Method to update virus definitions, communication occurs between managed computers to verify whether virus definitions files are current. Communication occurs in the following ways:

- Primary servers communicate with their secondary servers to verify that virus definitions are current. If a primary server finds that virus definitions on secondary servers are not current, it pushes new virus definitions files to those computers.
- Parent servers communicate with the clients that they manage to verify whether virus definitions are current. If a parent server finds that virus definitions on managed clients are not current, it pushes new virus definitions and configuration data to those computers.

When you use LiveUpdate to update virus definitions, communication occurs automatically when LiveUpdate is initiated on the client. During a scheduled or manual LiveUpdate session, clients communicate with an internal LiveUpdate server or the Symantec LiveUpdate server to verify that their virus definitions are current. If virus definitions are not current, the client pulls virus definitions updates from the contacted LiveUpdate server.

Communication for status information

Symantec AntiVirus clients provide status information to their parent servers. By default, a client sends a small packet (less than 1 KB) called a keep alive packet to its parent server every 60 minutes. The packet contains configuration information about that client. When a client's parent server receives a keep alive packet that indicates that the client does not have current virus definitions files or configuration data, the parent server pushes the appropriate files to that client.

Note: Symantec AntiVirus uses the User Datagram Protocol (UDP) for client-server communication. Because some router policies block UDP packets when they are sent between routers, you may need a computer that is running Symantec AntiVirus server on both sides of each router in your network.

Roaming client communication

Roaming client communication ensures that a roaming-enabled computer connects to the best parent. Roaming client communication employs the following four components:

- A list that specifies the servers to which roaming clients can connect. This list is merged into the registry of each Symantec AntiVirus roaming client.
- A list that describes the hierarchy of parent servers in your network. Servers at the top level cover the widest geographic area with each subsequent level covering more specific locations.
- The roaming client administration application (RoamAdmn.exe) that you roll out to each roaming server.
- A Symantec AntiVirus client installation with roaming support enabled (by use of a registry switch).

Using RoamAdmn.exe, the hierarchical server list is merged into the registry of each roaming server. When a roaming-enabled computer starts, it examines its list of roaming parents, and measures the access time for each parent. The client selects the best parent, based on access time, number of computers that are managed by that parent, and ranking within the server list. The Symantec AntiVirus service periodically verifies that the connection is still active, and that it is still the best available connection based on the list of servers.

How alerting works

Alert Management System^2 (AMS^2), provides a centralized alerting capability when you manage Symantec AntiVirus.

AMS alerting

The AMS^2 console is a Symantec System Center component that supports alerts from computers that are running AMS^2 server and client.

AMS^2 can process notifications that are generated by Symantec AntiVirus servers and clients through the following alert methods:

- Message Box
- Broadcast
- Send Internet Mail
- Send Page
- Run Program

- Write to Windows NT Event Log
- Send SNMP Trap
- Load an NLM

AMS^2 server is installed by default when the Symantec AntiVirus server program is installed using the AV Server Rollout tool. Managed antivirus clients do not require AMS^2 client to generate alerts.

When you install an unmanaged Symantec AntiVirus client, AMS^2 client is not installed by default. To install AMS^2 to an unmanaged client, you must install the stand-alone AMS^2 client software that is available on the Symantec AntiVirus CD.

How the Digital Immune System works

The Digital Immune System is a fully automated, closed-loop antivirus system that manages the entire antivirus process, including virus discovery, virus analysis, and deployment and repair of files that could not be repaired on a client computer. This automated system dramatically reduces the time between when a virus is found and when a repair is deployed, which decreases the severity of many threats.

The Digital Immune System works with the Central Quarantine and performs the following actions:

- Identifies and isolates viruses

  When a client computer configured to repair infected files cannot repair a specific file, it forwards the file first to the local Quarantine and then to the Central Quarantine Server where more current virus definitions may be available.
- Rescans the file and submits viruses to Symantec Security Response

  If the Central Quarantine has more current virus definitions than the submitting computer, it may be able to fix the file. If so, it pushes the newer definitions to the submitting computer. If the file cannot be repaired, it is sent to a Symantec Security Response gateway for further analysis.

- Analyzes submissions, and generates and tests repairs
  When the Digital Immune System receives a new submission, it analyzes the virus, generates the repair, and tests it. Then it builds new virus definitions files, including the new virus fingerprint, and returns the new virus definitions files to the gateway. Usually, this process occurs automatically; however, some cases require the intervention of Symantec Security Response.
- Deploys repairs
  The Quarantine Agent downloads the new virus definitions and installs them on the Central Quarantine Server. The updated definitions are then pushed to the submitting computer, if they are needed.

For details about configuring the Central Quarantine and using the Digital Immune System, see the *Symantec Central Quarantine Administrator's Guide*.

What you can do with Symantec AntiVirus

You can use Symantec AntiVirus to accomplish the following key protection tasks on your network servers and workstations:

- Deploy protection efficiently.
- Protect against viruses.
- Protect against other threats.
- Manage Symantec AntiVirus clients based on their connectivity.
- Centrally manage and update security.
- Ensure that remote clients comply with your security policy.
- Verify security status.
- Establish and enforce policies.
- View history and event log data.

Deploy protection efficiently

Symantec AntiVirus uses Microsoft Windows Installer (.msi) technology for the installation and deployment of Symantec AntiVirus.

Windows Installer files support a wide variety of configuration and installation options for Symantec AntiVirus client and server installations. In addition to the standard Windows Installer options, Symantec AntiVirus includes a set of command-line options that can be used to customize the installation. The use of Windows Installer technology provides reduced deployment size, a smaller installation footprint, fully customizable security options, support for a broad variety of management and deployment environments, and support for in-field patches for security updates and feature upgrades.

When you use Windows Installer packages, you can deploy Symantec AntiVirus with any of the following:

- The Symantec System Center
- Web-based installation
- Network logon scripts
- Third-party deployment tools, such as Microsoft Active Directory, Tivoli, Microsoft Systems Management Server (SMS), Novell ManageWise ZENworks, and Microsoft IntelliMirror
- Symantec Packager deployment tool (part of Symantec Packager)

Note: Symantec Packager is included with this release of Symantec AntiVirus as an unsupported tool. For more information, see *Using Symantec Packager with Symantec AntiVirus* (pkgrinfo.pdf) in the Symantec Packager folder on the Symantec AntiVirus CD.

Protect against viruses

You can protect against virus outbreaks by configuring scanning criteria and scheduling scans for all computers running Symantec AntiVirus. To protect your network, you can do the following:

- Verify that all of the computers running Symantec AntiVirus have the latest virus definitions files.
- Enable expanded threat scanning for manual and scheduled scans to detect threats other than viruses, such as adware and spyware.
- Set specific scanning options for specific computers, for example, computers that are managed by the same parent server or belong to the same server or client group.
- Configure supported 32-bit and 64-bit computers that are running the Symantec AntiVirus client to scan email attachments for the following applications:
  - Lotus Notes clients
  - Microsoft Exchange/Outlook clients that use Messaging Application Programming Interface (MAPI)

- Configure supported 32-bit and 64-bit computers that are running the Symantec AntiVirus client to scan email body text and attachments that are sent or received using the POP3 or SMTP protocols.
- Enable outbound email heuristics scanning, which uses Bloodhound Virus Detection to identify threats that may be contained in outgoing messages. Scanning outgoing email messages helps to prevent the spread of threats such as worms that can use email clients to replicate and distribute themselves across a network.
- Configure computers that are running Symantec AntiVirus to automatically forward unrepaired infected files to a Central Quarantine Server.
- Perform a threat trend analysis. You can use the results to improve security, for example, by changing configuration options for higher risk clients or disallowing trackware to run on computers. Threat History and Event Log data also can be exported to many third-party reporting systems.

Symantec AntiVirus client users may be allowed to do the following:

- Create and save startup scans that run automatically when the computer starts.
- Create custom scans that run manually on the client.
- Schedule scans of specific drives, folders, and files to run automatically at a specific time and date.

Protect against other threats

Symantec AntiVirus can expand the types of threats for which it scans to include the following categories:

- Spyware
- Adware
- Dialers
- Joke programs
- Remote access programs
- Hack tools
- Trackware

Manage Symantec AntiVirus clients based on their connectivity

Symantec AntiVirus provides protection for clients with varying levels of network connectivity. Client connectivity is classified as follows:

- Fully managed clients attach and log on to the network on a regular basis. They are managed by the Symantec System Center console.
- Sometimes managed clients typically are mobile or telecommuting users who use a virtual private network (VPN) to connect to the network. They share most of the characteristics of managed clients and are managed by the Symantec System Center console.
- Lightly managed clients are typically mobile computers that do not connect to the network, but have email. They are configured outside of the Symantec System Center through a configurations file (Grc.dat).
- Unmanaged clients do not connect to the network and have no parent server with which to communicate. They use a configurations file during installation and are self-managed.
- Roaming clients are typically mobile computers that connect to a parent server while traveling. They are managed using RoamAdmn.exe and SavRoam.exe.

Centrally manage and update security

The Symantec System Center is a management framework used for controlling Symantec AntiVirus components, solving problems, and performing routine maintenance.

From the Symantec System Center, you can do the following:

- Discover computers that are running Symantec AntiVirus server.
- Find computers that are not running antivirus protection.
- Roll out the installation of Symantec AntiVirus to supported Windows workstations and network servers.
- Set up and administer Symantec AntiVirus server groups and client groups.
- Configure antivirus protection.
- Manage events by using alerts.
- Perform remote operations, such as threat scans and virus definitions files updates.

If your site has a decentralized administration structure with multiple administrators, you can run as many copies of the Symantec System Center console as you need. Because each server group has its own password, you can divide or share administrative duties in any way that works best for you.

Ensure that remote clients comply with your security policy

Symantec VPN Sentry reduces exposure to threats by preventing users with nonsecure computers from connecting to the corporate network. Computers attempting to access your corporate network must meet your policy requirements for Symantec AntiVirus server and Symantec AntiVirus client.

You can use Symantec VPN Sentry on remote computers that connect to your network through a virtual private network (VPN) connection.

The SymSentry folder on the Symantec AntiVirus CD includes vendor-specific Symantec VPN Sentry plug-ins and documentation. Other vendors support Symantec VPN Sentry client compliancy. Check with your vendor to determine if they provide Symantec VPN Sentry support. For more information on Symantec VPN Sentry, see the SymSentry folder on the Symantec AntiVirus CD.

A security policy may include the following requirements:

- Auto-Protect is enabled.
- Auto-Protect heuristic virus scanning is enabled and at least at the specified level.
- Auto-Protect is configured to scan on specified types of file access.
- A LiveUpdate session completed successfully within a specified number of days.
- The installed Symantec AntiVirus version is at least a specified version.
- Virus definitions files are no older than a specified maximum age.
- A specified scan ran within the last (n) days.
- The Microsoft Exchange/Outlook plug-in scanner is installed and enabled.
- The Lotus Notes plug-in scanner is installed and enabled.

You can configure Symantec VPN Sentry to deny a computer access to your network until it is remediated with the required software or settings. Once the computer complies with your security policy, Symantec VPN Sentry can allow the computer to access the network.

You can remediate some compliancy issues automatically (for example, you can enable Auto-Protect on a client). Other compliancy issues may require a manual resolution (for example, a computer may need to update to a compliant Symantec AntiVirus version).

Verify security status

Using the Symantec System Center console, you can select and view the protection settings for any managed computer that is running Symantec AntiVirus. Managed computers appear in the right pane of the console when their parent servers are selected in the tree.

Establish and enforce policies

You can establish and enforce the following policies to control the Symantec AntiVirus user experience:

- You can lock configuration settings such as Auto-Protect scanning to ensure that your clients remain protected from viruses at all times.
- You can tamper-protect the Windows registry values that Symantec AntiVirus uses, and receive notifications when specific registry keys are modified. This is the default setting.
- You can password-protect server groups so that changes to server and client settings can be made by authorized staff only.

View history and event log data

The Symantec System Center console offers basic reporting tools for history and event log data. Reports are based on Symantec AntiVirus servers, server groups, or clients. You can specify a time range in which to filter the data that appears in the report. For example, you might want to view only those scans that ran within the last seven days. For more complex reports, you can export the data as a comma-delimited file for use with a third-party reporting tool.

Where to get more information about Symantec AntiVirus

Sources of information on using Symantec AntiVirus include the following:

- *Symantec AntiVirus Administrator’s Guide*
- *Symantec AntiVirus Reference Guide*
- *Symantec AntiVirus Client Guide*
- *LiveUpdate Administrator’s Guide*
- *Symantec Central Quarantine Administrator’s Guide*
- Online Help that contains all of the content found in the above guides and more

The primary documentation is available in the Docs folder on the Symantec AntiVirus CD. Some individual component folders contain component-specific documentation. Updates to the documentation are available from the Symantec Technical Support and Platinum Support Web sites.

Additional information is available from the Symantec Web sites listed in Table 1-3.

Table 1-3 Symantec Web sites

Types of information	Web address
Public Knowledge Base Releases and updates Manuals and documentation Contact options	http://www.symantec.com/techsupp/enterprise/
Virus and other threat information and updates	http://securityresponse.symantec.com
Product news and updates	http://enterprisesecurity.symantec.com
Platinum Support Web access	https://www-secure.symantec.com/platinum/

Chapter 2

Planning the installation

This chapter includes the following topics:

Installation overview

Before you can install Symantec AntiVirus you should plan appropriately.

Typical installation tasks

To install a Symantec AntiVirus solution on your network you would typically perform the following steps:

- Install the Symantec System Center and console components.
  See “About Symantec System Center management components” on page 42.
- Install Symantec AntiVirus server.
  If a Windows-based network server is not used for administration tasks, install the Symantec AntiVirus client program.
  See “Server installation methods” on page 44.
- Designate the server as a primary server.

- Install Symantec AntiVirus clients.
  See "Client installation methods" on page 45.
- Install the following optional administration tools:
  - Central Quarantine Server
  - Quarantine Console snap-in
  - LiveUpdate Administrator
- Update virus definitions.
  See "Methods for updating virus definitions files" on page 50.

Installation guidelines

Although there are many variations in the size and complexity of every installation, the following general guidelines apply to most environments:

- Create a server group for each site location.
- Designate a primary server for each server group.
- Install Symantec AntiVirus server on a computer with a single NIC. Select systems with low to moderate use for the Symantec AntiVirus primary server and any secondary servers.
- Use name resolution throughout the networking environment. WINS is required for the Discovery Service and one or more of the following services are also required: DNS, HOST, or LMHOST.
  NetBIOS is not recommended for name resolution.
- Use a computer running Windows NT or Windows 2000 as a primary server.

About creating an installation plan

Before you begin to install Symantec AntiVirus, you should create an installation plan that addresses the following issues:

- Which management tools do I need to install?
- Which server installation methods will I use?
- Which computers will I use as primary servers, secondary servers, and parent servers?
- Which client installation methods will I use?
- How will I perform remote installations?

- How will I update virus definitions?
- How will I set up my test environment before rolling out to my production environment?

You should review the preinstallation considerations and installation requirements to learn about any issues that will affect your planning decisions.

See "General preinstallation considerations" on page 57.

See "Installation requirements" on page 69.

How to implement a solution

You can use Symantec AntiVirus in environments that range in size from a small business to a large enterprise. Different sized environments must consider how they are going to perform the following tasks:

- Rolling out the installation
- Managing alerting
- Protecting against viruses and other threats
- Updating virus definitions
- Ensuring client compliancy

To understand how you can best install Symantec AntiVirus and perform management operations after installation, you may want to review scenarios that describe how Symantec AntiVirus is implemented in different sized organizations.

For detailed information on how Symantec AntiVirus is implemented in an environment that matches the profile of your organization, see the *Symantec AntiVirus Reference Guide*.

About Symantec System Center management components

If you plan to use the Symantec System Center for management services, including the rollout of the installation to managed computers, it is important to have an understanding of the management components and issues related to their installation. During installation of the Symantec System Center, the management components are installed by default, unless you specify otherwise.

Table 2-1 lists and describes Symantec System Center management components.

Table 2-1 Symantec System Center management components

Component	Description	Overview
The Symantec System Center console	The Symantec System Center is the console that you use to administer managed Symantec products. The Symantec System Center is a stand-alone application that runs under Microsoft Management Console.	■ Install the Symantec System Center console to the computers from which you plan to manage Symantec AntiVirus. ■ Install to at least one computer to view and administer your network. If your organization is large or you work out of several offices, you can install the Symantec System Center to as many computers as you need. Rerun the installation program and select the appropriate option. ■ The Symantec System Center does not need to be installed on a network server or an antivirus server.
Alert Management System^2 (AMS^2) console	The AMS^2 console provides alerts from AMS^2 clients and servers. When you install the AMS^2 console, you can configure alert actions for Symantec AntiVirus servers that have the AMS^2 service installed. When a problem occurs, AMS^2 can send alerts through a pager, an email message, and other means.	■ Install the AMS^2 console to the same computer on which the Symantec System Center console is installed. ■ Install the AMS^2 service to one or more primary servers on which Symantec AntiVirus server is installed. ■ If you choose not to install AMS^2, you can use the notification and logging mechanisms that are available from the Symantec System Center. ■ If you plan to implement Symantec Enterprise Security alerting instead of AMS^2, you do not need to install AMS^2.

Table 2-1 Symantec System Center management components

Component	Description	Overview
Symantec AntiVirus snap-in	This management snap-in for the Symantec System Center lets you manage Symantec AntiVirus on workstations and network servers.	Install this component to do the following from the Symantec System Center: ■ Set up and administer Symantec AntiVirus server and client groups. ■ Manage antivirus protection on computers that are running Symantec AntiVirus. ■ Configure groups of computers that are running Symantec AntiVirus. ■ Manage events. ■ Configure alerts. ■ Perform remote operations, such as virus scans and virus definitions files updates.
NT Client Install tool	This tool lets you remotely install Symantec AntiVirus client to one or more Windows NT-based computers. You can also run this tool from the Symantec AntiVirus CD.	Install this component to manage remote client installations.
AV Server Rollout tool	This tool lets you remotely install Symantec AntiVirus server to the Windows NT-based computers and NetWare servers that you select. You can also run this tool from the Symantec AntiVirus CD.	Install this component to manage remote server installations from the Symantec System Center.

See “Installing the Symantec System Center” on page 91.

Server installation methods

You can install Symantec AntiVirus servers using any of the methods that are listed in Table 2-2. You can use any combination of methods that suits your network environment.

Table 2-2 Server installation methods

Method	Description	Preparation
Push	You can push a Symantec AntiVirus server installation directly from the Symantec AntiVirus CD or from the Symantec System Center.	Install the Symantec System Center with the Symantec AntiVirus snap-in and the AV Server Rollout tool to push the server installation from the Symantec System Center.
Windows Installer (.msi) deployment	You can create and deploy an installation package using tools that are compatible with Windows Installer. Symantec AntiVirus uses Windows Installer technology for all client and server installations. Symantec AntiVirus utilizes the standard Windows Installer deployment options provided by Microsoft. To use this method, you must be familiar with creating and deploying Windows Installer programs.	■ Create a custom .msi installation package using the components and options specific to Symantec AntiVirus. See "Windows Installer (.msi) command-line reference" on page 161. ■ Determine a method for distributing and executing the package.
Self-extracting executable	You can create a package with Symantec Packager that includes a preconfigured Windows Installer package or set of packages. Customizing the Windows Installer installation packages using Symantec Packager is not supported. Distribute and execute a package to install Symantec AntiVirus directly onto a computer. **Note:** Symantec Packager is included with this release of Symantec AntiVirus as an unsupported tool. For more information, see *Using Symantec Packager with Symantec AntiVirus* (pkgrinfo.pdf) in the Symantec Packager folder on the Symantec AntiVirus CD.	■ Create a custom Symantec AntiVirus server installation package, if desired. ■ Determine a method for distributing and executing the package.

See "About Symantec AntiVirus server installation" on page 108.

Client installation methods

You can install a Symantec AntiVirus client using any of the methods that are listed in Table 2-3. You can use any combination of methods that suits your network environment.

Table 2-3 Client installation methods

Method	Description	Preparation
Push	You can push a Symantec AntiVirus client installation directly from the Symantec AntiVirus CD or from the Symantec System Center. This method lets you install clients on computers running supported Microsoft Windows operating systems without giving users administrative rights to their computers.	Install the Symantec System Center with the antivirus management snap-in and the NT Client Install tool to push the client installation from the Symantec System Center.
Logon script	For legacy client installation information, see the *Norton AntiVirus Corporate Edition Implementation Guide* that came with your legacy software.	Use your network administration tools to associate users with the logon script.
From a server	You can run a Symantec AntiVirus client installation package from the Symantec AntiVirus server that you want to act as a parent server.	■ Install Symantec AntiVirus server. ■ Have users map a drive to the VPHOME\clt-inst\WIN32 share on Symantec AntiVirus server to ensure a successful installation.
Web	Users download a client installation package from an internal Web server, and then run it. This option is available for computers that are running supported Windows operating systems.	■ Ensure that the Web server meets the minimum requirements. ■ Prepare the internal Web server for deployment. ■ Copy a preconfigured client installation package to the Web server or create a custom installation package, if desired. ■ For legacy client installation information, see the *Norton AntiVirus Corporate Edition Implementation Guide* that came with your legacy software.

Table 2-3 Client installation methods

Method	Description	Preparation
Local	You can run the installation directly from the Symantec AntiVirus CD. This is the primary installation method supported for 64-bit computers.	Copy the configurations file (Grc.dat) from the parent server to the client computer.
Third-party tools	You can use a variety of third-party installation tools to distribute the Windows Installer-based installation files.	■ See the documentation that came with your third-party installation tool for instructions on using the tool. ■ Create a custom .msi installation using the components and options specific to Symantec AntiVirus installation packages.
NetWare server automatic installations	You can configure Symantec AntiVirus to install automatically to your Windows clients from NetWare servers.	Install the Symantec AntiVirus server on the NetWare server.

See “About Symantec AntiVirus client installation” on page 132.

Types of Symantec AntiVirus clients

Symantec AntiVirus manages protection for client computers based on their network connectivity.

Table 2-4 categorizes the types of client computers that you can manage and lists how they are managed.

Table 2-4 Symantec AntiVirus client types

Client type	Description	Managed by
Fully managed	These clients attach and log on to the network on a regular basis. Managed clients can do the following: ■ Regularly communicate with a parent server and download configuration and virus definitions files updates as often as necessary. ■ Appear in the Symantec System Center under their parent servers. ■ Immediately send alerts if Symantec AntiVirus detects a virus or other threat. Client log information is also available in the Symantec System Center. ■ Have their configuration settings locked in the Symantec System Center so that users cannot change them. ■ Automatically install to a user's hard drive through logon scripts. ■ Receive software installations that are pushed from the Symantec System Center.	The Symantec System Center console
Sometimes managed	These clients typically are mobile or telecommuting users who use a VPN to connect to the network. They share most managed client characteristics. Settings that you lock remain locked even if the client computer is not connected to the network. The next time that these clients log on to the network, they receive any new configuration data and the latest virus definitions files updates. By default, if a parent server does not communicate with a sometimes managed client for 30 days, the icon is removed from the Symantec System Center display.	The Symantec System Center console

Table 2-4 Symantec AntiVirus client types

Client type	Description	Managed by
Lightly managed	These clients are configured outside the Symantec System Center console through a configurations file (Grc.dat), and are otherwise not managed. Lightly managed clients are typically mobile computers that do not connect to the network, but have email. If a lightly managed client requires a configuration change, you can create a new configurations file and copy it to the client. You can change the configuration of lightly managed clients by pushing a new configurations file to clients using third-party software.	Configurations file (Grc.dat)
Unmanaged	These clients do not connect to the network and have no parent server with which to communicate. They will not appear in the Symantec System Center even if they are later connected to the network. These clients need to download their own virus definitions updates. LiveUpdate is built in to each Windows client so that it can automatically get new virus definitions files updates.	■ Configurations file (Grc.dat) during installation ■ Self-managed
Roaming	These clients are typically mobile computers that dynamically connect to a parent server while traveling. These clients use Roaming Client Support, which detects the new location and reassigns the user's laptop to the best parent server. Roaming Client Support also lets you balance the load among a pool of servers that are equal in connection speed and proximity based on the client load on the computers.	■ RoamAdmn.exe ■ SavRoam.exe

About administration tools

If you plan to implement a security solution that includes, for example, a Central Quarantine Server or an internal LiveUpdate server, you need to install the appropriate administrator tools.

Table 2-5 lists and describes the administration tools.

Table 2-5 Administration tools

Administration tool	Description	Preparation
Quarantine Console snap-in	Lets you manage the Central Quarantine Server from the Symantec System Center.	Install on the computer on which the Symantec System Center is installed.
Central Quarantine Server	Allows antivirus clients to automatically forward infected items to the Central Quarantine, where they can be submitted to Symantec Security Response by email or the Internet for analysis. If a new virus is identified, updated virus definitions are returned to the submitting computer. For more information, see the *Symantec Central Quarantine Administrator's Guide*.	■ Install on the computer on which you want to run the Central Quarantine Server. ■ The Central Quarantine Server and the Central Quarantine Console can be installed on the same or different supported Windows computers.
Custom Content Publishing Application	You can use LiveUpdate to automatically distribute and update content of virtually any type, including documents and program files. You can work with Symantec content, or any content that is related to other products or services. You can target content to classes of client computers based on the target client's network location, computer name, registry information, files currently installed on the computer, and other parameters. Using the Custom Content Publishing Application (CCPA), you create, modify, and publish updates that are uploaded to the Central LiveUpdate server. When the LiveUpdate client runs, it looks for custom content packages in addition to LiveUpdate virus definitions and product updates, and authenticates the package to determine if it can be trusted. See the *LiveUpdate Administrator's Guide*.	Install the Custom Content Publishing Application (CCPA) on a computer that is running a supported Windows operating system.
LiveUpdate Administrator	Lets you configure one or more intranet FTP, HTTP, or LAN servers to act as internal LiveUpdate servers.	Install on a Windows NT computer that is running the Symantec AntiVirus server program.

Methods for updating virus definitions files

Symantec AntiVirus provides several methods for keeping the virus definitions files current across all networked and non-networked computers. The information in Table 2-6 will help you understand the various methods, the types of clients to which they apply, and considerations for using each method.

Table 2-6 lists the update methods and the types of clients on which to use them.

Table 2-6 Virus definitions files update methods

Update method	Description
Virus Definition Transport Method	Use with fully managed and sometimes managed computers. This method allows primary servers to push updated virus definitions to secondary servers and secondary servers to the clients that they manage. Primary servers may receive updated virus definitions from an internal LiveUpdate server, if you have one, or the Symantec LiveUpdate server. If you use a single computer on your network as a source for updating virus definitions, you can reduce network exposure to the Internet. Additionally, if the computer is configured as an internal LiveUpdate server, you can automate the procedure for updating virus definitions. For a large network, you can create more than one internal LiveUpdate server for failover protection. When you are updating virus definitions files, plan to stagger the update schedule to minimize network traffic or schedule updates during off-peak hours. **Note:** This method is not supported on 64-bit computers.

Table 2-6 Virus definitions files update methods

Update method	Description
LiveUpdate	Use with fully managed, sometimes managed, lightly managed, and unmanaged computers. This method allows Symantec AntiVirus servers or clients to initiate updates through the LiveUpdate feature of Symantec AntiVirus and receive new virus definitions files from an internal LiveUpdate server, if you have one, or the Symantec LiveUpdate server. For fully managed and sometimes managed computers, LiveUpdate configurations can be pushed directly from the Symantec System Center. To enable unmanaged computers to get virus definitions updates from an internal LiveUpdate server, prepare a custom configuration file named Liveupdt.hst and copy it into the correct folder on each unmanaged computer. **Note:** LiveUpdate is the only virus definitions files update method supported on 64-bit computers.
Central Quarantine polling	Use with managed and unmanaged computers. This method uses the Central Quarantine Server, which polls the Symantec Digital Immune System gateway for new virus definitions files and automatically pushes them to the computers whose definitions are out of date. Central Quarantine polling uses the Virus Definition Transport Method to distribute the virus definitions files to managed computers. To prepare for Central Quarantine polling, do the following: ■ Install the Central Quarantine Server software. ■ Install the Central Quarantine Console on a computer with the Symantec System Center. ■ Review the polling frequency setting (the default is three times a day) and the virus definitions files installation settings in the Central Quarantine Console. **Note:** This method is not supported on 64-bit computers. See the *Symantec Central Quarantine Administrator's Guide* on the Symantec AntiVirus CD.

Table 2-6 Virus definitions files update methods

Update method	Description
Intelligent Updater	Use with lightly managed and unmanaged computers. This method uses Intelligent Updater files, which are self-extracting executable files that contain virus definitions. They are available for download from the Symantec Security Response Web site. If you choose this method, you must decide how you want to distribute the Intelligent Updater files, for example, distributing them on CDs to laptop users. **Note:** This method is not supported on 64-bit computers.

Best practice: Piloting Symantec AntiVirus in a lab setting

Before you begin a full-scale installation, you should install Symantec AntiVirus in a nonproduction lab setting. You can use this evaluation period to address any installation issues before a full deployment to your production environment.

Before you begin the pilot, you may want to review preinstallation considerations and installation requirements.

See "General preinstallation considerations" on page 57.

See "Installation requirements" on page 69.

Simulating a realistic network environment in a lab setting

When you test Symantec AntiVirus server and client components in a lab setting, you should do the following:

- Create a realistic and representative network environment.
  See "How to create a representative network environment" on page 53.
- Test Symantec AntiVirus server installations.
  See "Testing Symantec AntiVirus client installations" on page 54.
- Obtain a virus test file.
  See "Obtaining a virus test file" on page 54.
- Test Symantec AntiVirus client installations.
  See "Testing Symantec AntiVirus client installations" on page 54.

How to create a representative network environment

Table 2-7 describes how to get the most out of a trial in which you test Symantec AntiVirus servers.

Table 2-7 Creating a representative network environment

Task	Description
Hardware configuration	Set up your hardware to at least the minimum requirements needed.
Installation	■ Install to at least two Symantec AntiVirus servers, mixing Windows NT-based and NetWare computers (if needed). ■ Perform a complete installation to each server, including AMS^2 (if needed). ■ Install the Symantec System Center to at least one computer that is using a 32-bit operating system. ■ Install to connected and stand-alone computers if necessary. ■ Match client to server operating system combinations (for example, a Windows NT workstation logging on to NetWare servers).
Communication	■ Match the communication protocols in your test environment to those in your production environment. Install to all operating systems that you expect to use. ■ If your network uses routers, include a router in your test environment (this is particularly important for mixed protocol environments).
Management	■ Create at least one server group that contains two or more servers. ■ Create at least one client group that contains two or more Symantec AntiVirus clients.

Note: If you are using a Windows NT Workstation 4.0 computer in a lab setting as a Symantec AntiVirus server, the maximum number of computers that can simultaneously connect to a Windows NT Workstation 4.0 is 10. This Microsoft-imposed limitation does not limit TCP connections that can be made to a computer, but affects only file shares, named pipes, and so on (anything that requires the SERVER service). Symantec AntiVirus can have as many inbound connections as it needs to function properly. To resolve connectivity problems without losing the service's self-tuning capability, you can lower the AutoDisconnect time by changing the AutoDisconnect time registry key. For more information, see the Microsoft Knowledge Base.

Testing Symantec AntiVirus server installations

After you have installed Symantec AntiVirus servers, complete the following tasks:

- Configure the different scans for maximum protection (all files, all drives, and so on).
- Test virus definitions file downloads and server-to-server updates.
- Create a virus test file (not a real virus) to see how the virus-detecting mechanisms work without introducing a real virus on your computer.
  See "Obtaining a virus test file" on page 54.
- Let scheduled scans and other automated functions run for several days.
- Verify that the Symantec System Center can view servers on both sides of routers.
  See "Required protocols" on page 69.
- Verify that log files and reports accurately reflect the expected data.

Obtaining a virus test file

You can verify virus detection, logging, and alert functionality by obtaining a virus test file from the following Web site:

http://www.eicar.org

From the Web site, you can download the eicar.com file. This file is not a virus, but it will be detected as the eicar.com (or similar) virus. You must disable Auto-Protect file protection temporarily before saving the file.

Testing Symantec AntiVirus client installations

After you have installed Symantec AntiVirus to the computers in your lab environment, complete the following tasks:

- Configure the different scans for maximum protection (all files, all drives, and so on).
- Test virus definitions file downloads.
- Obtain a virus test file to trigger the alerting system.
  See "Obtaining a virus test file" on page 54.
- Let scheduled scans and other automated functions run for several days.
- Verify that the Symantec System Center can view Symantec AntiVirus clients on both sides of routers.
  See "Required protocols" on page 69.

- Verify that connected Symantec AntiVirus clients appear in the Symantec System Center console under the correct parent server.
- Lock some Symantec AntiVirus client scanning parameters using the Symantec System Center and verify that users cannot change these settings.
- Launch a virus sweep and verify that the Symantec AntiVirus client scans take place.
- Verify that log files and reports reflect the expected data.

Chapter 3

Preparing to install Symantec AntiVirus

This chapter includes the following topics:

- General preinstallation considerations
- Preparing for Symantec AntiVirus server installation
- Preparing for Symantec AntiVirus client installation
- Installation requirements

General preinstallation considerations

Before you install Symantec AntiVirus, review the following topics:

- How to prepare for the Symantec System Center installation
- About customizing the client and server installation files using Windows Installer options
- About configuring user rights with Active Directory
- About setting administrative rights to target computers

How to prepare for the Symantec System Center installation

Before you install the Symantec System Center, on the computer to which you are installing the Symantec System Center, you should uninstall the following:

- Any earlier versions of the Symantec System Center
- Any earlier versions of Symantec AntiVirus (including any versions of LANDesk Virus Protect)

The Symantec System Center can manage any earlier supported versions of Symantec AntiVirus, but the computer that is running the Symantec System Center must be using the current version of Symantec AntiVirus. You can install the Symantec System Center console to as many computers as you need to manage Symantec AntiVirus.

About customizing the client and server installation files using Windows Installer options

The Symantec AntiVirus client and server installation packages are Windows Installer (.msi) files that are fully configurable and deployable using the standard Windows Installer options. You can use environment management tools that support .msi deployment, such as Active Directory or Tivoli, to install clients on your network.

See "Windows Installer (.msi) command-line reference" on page 161.

About configuring user rights with Active Directory

If you are using Active Directory to manage Windows-based computers on your network, you can create a Group Policy that provides the necessary user rights to install Symantec AntiVirus.

For more information on using Active Directory, see the Active Directory documentation provided by Microsoft.

About setting administrative rights to target computers

To install Symantec AntiVirus server to a computer running supported Windows operating systems, you must have administrator rights to the computer or to the Windows NT domain to which the computer belongs, and log on as administrator. The Symantec AntiVirus server installation program launches a second installation program on the computer to create and start services and to modify the registry.

If you do not want to provide users with administrative rights to their own computers, use the NT Client Install tool to remotely install Symantec AntiVirus client to computers that are running supported Windows operating systems. To run the NT Client Install tool, you must have local administrative rights to the computers to which you are installing the program.

See "Installing Symantec AntiVirus clients" on page 129.

Preparing for Symantec AntiVirus server installation

To ensure a successful Symantec AntiVirus server rollout, review the following considerations:

- Symantec AntiVirus server installation options
- About required restarts
- Locating servers across routers during installation
- Verifying network access and privileges
- Installation order for Citrix Metaframe on Terminal Server
- Installing to NetWare servers
- Terminal Server protection
- Preventing user-launched virus scans

Symantec AntiVirus server installation options

The computers on which you install Symantec AntiVirus server will be added to a single server group. You can create additional server groups from the Symantec System Center console and use a drag-and-drop operation to populate them.

When you install Symantec AntiVirus server, the setup program copies files to the selected Windows NT-based computers. Then a second setup program (Vpremote.exe), which requires no user input, runs on the computer to create and start Symantec AntiVirus services and modify the registry.

The installation program installs Symantec AntiVirus NLMs to the supported NetWare servers that you select and installs services to the supported Windows computers that you select.

About required restarts

The following are a few instances in which a restart is necessary:

- Installing AMS^2 to a Windows NT computer.

  Restart the computer after the installation program has completed in order for AMS^2 to run.
- Updating Symantec AntiVirus files on a Windows NT computer (for example, when you apply a service release), in which case some files might be in use.

  Restart the computer to replace the older files.

As you install or update Symantec AntiVirus, the installation program displays a status for each server. The status reports the progress of the installation or update, alerts you to any errors, and prompts you for any required action. After an installation or update, if the installation program needs to replace any files that are in use, the status is Restart necessary for Windows NT computers.

Locating servers across routers during installation

You can browse to find the computers on which you want to install Symantec AntiVirus server. Computers that are located across routers might be difficult to find. To verify that you can see a computer when you run the Symantec AntiVirus server installation program, try mapping a drive to the server using Windows Explorer. If you can see a computer in Windows Explorer, you should see the computer when you run the Symantec AntiVirus server installation program.

Browsing requires the use of the Windows Internet Name Service (WINS). For computers that are located in a non-WINS environment (such as a native Windows 2000 network that uses the LDAP or DNS protocol), you must create a text file with IP addresses and then import it to be able to install to those computers.

Creating a text file with IP addresses to import

You can create a text file of the IP addresses of computers that are located in a non-WINS, Windows NT-based environment. During installation, you can import the text file and add the listed computers to the computers on which you want to install the server program.

Note: The Import feature is designed for use with supported Windows NT-based operating systems only. It is not intended for use with NetWare.

To create a text file with IP addresses to import

1. In a text editor (such as Notepad), create a new text file.
2. Type the IP address of each computer that you want to import on a separate line.
   For example:
   192.168.1.1
   192.168.1.2
   192.168.1.3
   You can comment out IP addresses that you do not want to import with a semicolon (;) or colon (:). For example, if you included addresses in your list for computers that are on a subnet that you know is down, you can comment them out to eliminate errors.
3. Save the file to a location that you can access when you run the server installation program.

Verifying network access and privileges

Review the following before installing the Symantec AntiVirus server program:

- The computer that you use to run the Symantec AntiVirus server installation program should have the appropriate network clients and protocols running (IP and IPX/IPX). This allows you to see all of the NetWare and Windows NT computers on which you want to install Symantec AntiVirus.
- Sharing must be enabled on the Windows NT computer on which you install Symantec AntiVirus server. The installation program uses the default NT shares such as c$ and admin$. When you install Windows NT, these shares are enabled by default. If you changed the share names or disabled sharing to the default shares, the installation program cannot complete the Symantec AntiVirus server installation.
- If you log on to a Windows NT/2000 domain and are put into a regular domain group without administrator rights over the local computer, you cannot install.

To reestablish the credential with the local computer

◆ At the command prompt, type the following:

```
net use \\machinename\ipc$/user:username password
```

Use this command to install if you are a local administrator with a different password than the domain administrator.

The rights that you need to install to server and client computers depend on the server platform and version.

How to deploy to a target computer without granting administrator privileges

You can deploy an installation that does not require administrator privileges using the Microsoft Management Console. Symantec AntiVirus client and server installations are Windows Installer packages, which means that you can use elevated privilege settings to enable installation on a target computer without granting administrator privileges. For more information on enabling elevated privileges during installation for Windows Installer components, see the Microsoft Management Console documentation.

Installation order for Citrix Metaframe on Terminal Server

Symantec AntiVirus does not support drive remapping for Citrix Metaframe. If you plan to use Citrix Metaframe and remap your drives, complete the following tasks in the order in which they are listed:

- Install Citrix Metaframe.
- Remap the drives.
- Install Symantec AntiVirus server or client.

Installing to NetWare servers

The Symantec AntiVirus server installation program copies NLMs and other files to one or more NetWare servers that you select. To install to NetWare servers, do the following:

- Before you begin installation, log on to all of the servers to which you want to install.
  To install to the NDS or bindery, you need administrator or supervisor rights.
- After you run the Symantec AntiVirus server installation program, go to the server console (or have rights to run RCONSOLE) to load the Symantec AntiVirus NLMs.
  You only need to do this manually the first time if you select the automatic startup option during Setup.

To load the Symantec AntiVirus NLMs the first time

◆ On the server console, type the following:

```
Load sys:\sav\vpstart.nlm /install
```

About installing to NetWare servers

If you are installing to any supported NetWare servers, the installation program prompts you to enter a user name and password for the NDS container that you select to hold logon scripts. Using the Symantec System Center and your network administration tools, you can enable the logon scripts to automate the Symantec AntiVirus client installation. You must have administrator-equivalent rights to the container that you designate.

About installing to a NetWare cluster

To install Symantec AntiVirus to a NetWare cluster, you install Symantec AntiVirus on each NetWare server in the cluster following the standard installation procedure for NetWare servers. Do not install Symantec AntiVirus to a volume.

See “Server installation methods” on page 107.

About installing into NDS

If you browse to an NDS object to which you are not authenticated, the installation program would normally prompt you to log on. However, some versions of the Novell client might not return a logon request, and in this case the installation program will time out or stop responding. To avoid this problem, log on to the NDS tree before running the installation program.

Protecting NetWare cluster servers and volumes

Symantec AntiVirus protects NetWare cluster servers and volumes by providing both Auto-Protect and manual scanning for each server in the cluster. Antivirus scanning of each volume in a cluster is managed by the server that has ownership of the volume. If the server with ownership of a cluster volume fails, NetWare transfers the ownership of the volume to another server in the cluster, which then automatically takes over the antivirus scanning tasks.

To protect NetWare cluster servers and volumes

◆ Launch Symantec AntiVirus after all volumes have been mounted and cluster services have been started in the Autoexec.ncf file.

Launching Symantec AntiVirus once these tasks are completed ensures that all volumes are detected.

Terminal Server protection

You can install either Symantec AntiVirus client or server to Terminal Servers. Symantec AntiVirus protection works on Terminal Servers in much the same way that it works on Windows NT/2000/2003 file servers. Alerting is the only difference.

Users who are logged on to the server console receive alerts. Users who are connected through a Terminal client session do not receive alerts.

How to view Terminal Servers from the Symantec System Center console

Terminal Servers appear the same as file servers in the console from which they are managed. Both types of servers are represented with the same icon in the Symantec System Center console.

Terminal Server and Terminal Services limitations

The following limitations apply to antivirus protection on Terminal Server and Terminal Services:

- Symantec AntiVirus does not protect mapped drives on computers that can be accessed by applications that are running during a session on Terminal Server.
- The file system Auto-Protect that is running on Terminal Server does not detect virus events, such as saving an infected file, that occur on local drives of Terminal Server clients.
- Symantec AntiVirus does not provide functionality to Terminal Server clients. For example, Symantec AntiVirus does not route alerts to the proper client session, or allow for the Symantec System Center to run within a session.
- Vptray.exe is the program that displays the antivirus Auto-Protect status in the system tray. Launching Vptray.exe each session is not feasible when you are scaling to a large user base due to the large footprint that is required for each session. Vptray.exe does not run if the session is remote but it does run on the Terminal Server console.
- When a user logs off of a remote Terminal session and the Auto-Protect setting to check floppy disks on computer shutdown is enabled, an unnecessary access is made to the floppy disk drive on the console. This setting is disabled by default.
- Session-specific information is not logged or included in virus alerts.

Preventing user-launched virus scans

You can prevent users from running manual scans in Terminal sessions by doing the following:

- Restrict the Windows Start menu and directories for Symantec AntiVirus to prevent users from running manual virus scans.
- Use the Application Security (AppSec) registration utility to restrict nonadministrator users to running only the programs that are included in an administrator-defined list of applications.

Prevent users from launching virus scans using AppSec

You can prevent users from running virus scans during Terminal sessions on a Windows NT 4.0 Terminal Server Edition server or a Windows 2000/2003 Terminal Services server using Application Security (AppSec).

AppSec installs automatically when you install Windows NT version 4.0 Terminal Server Edition. For Windows 2000/2003 Terminal Services, AppSec is included in the Windows 2000/2003 Server Resource Kit.

You must install both AppSec and the AppSec hotfix. You can find information about installing AppSec and the hotfix at:

http://www.microsoft.com/windows2000/techinfo/reskit/tools/hotfixes/appsec-o.asp

To prevent users from launching virus scans from a Windows NT Terminal Server

1. On the Terminal Server, on the Windows taskbar, click **Start** > **Programs** > **Administrative Tools** > **Application Security**.
2. In the Authorized Applications dialog box, in the Security group box, click **Enabled**.
   Users are denied access to any program that is not included in the Authorized Applications list, including the Symantec AntiVirus virus scanner.

To prevent users from launching virus scans from a Windows 2000/2003 Terminal Services server

1. On the Terminal Server, on the Windows taskbar, click **Start** > **Programs > Windows 2000 Resource Kit > Tools**.
2. Double-click **Alphabetized List of Tools**.

3. Click **Application Security**.
4. In the Authorized Applications dialog box, in the Security group box, click **Enabled**.

   Users are denied access to any program that is not included in the Authorized Applications list, including the Symantec AntiVirus virus scanner.

Preparing for Symantec AntiVirus client installation

To ensure a successful Symantec AntiVirus client rollout, review the following preinstallation considerations:

- About the Symantec AntiVirus client on a Terminal Server
- About Windows NT/2000 cluster server protection
- About required restarts
- About email support

About the Symantec AntiVirus client on a Terminal Server

The Symantec AntiVirus client program can be installed on a Terminal Server. The same considerations and limitations that apply to running the Symantec AntiVirus server on a Terminal Server apply to the Symantec AntiVirus client program.

See “Installation order for Citrix Metaframe on Terminal Server” on page 62.

See “Terminal Server protection” on page 64.

About Windows NT/2000 cluster server protection

You can protect and manage Windows NT/2000 cluster servers with Symantec AntiVirus.

To protect cluster servers, complete the following tasks:

- Install the Symantec AntiVirus client to each local computer that is part of the cluster server. Do not install to the shared drives.
- Roll out Symantec AntiVirus clients using the local server names rather than the shared cluster name.

Each Symantec AntiVirus client is managed separately and provides protection in the event of a failover. You can synchronize the manageability of the clients if they are managed by the same Symantec AntiVirus server and configuration is performed at the server level.

The shared drives are protected in real time by Auto-Protect on each computer when the computer has control of the drives. When control of the shared drives is passed to another computer, Auto-Protect on that computer automatically takes over the protection.

If a manual scan of the shared drives is being performed when a failover occurs, the scan does not restart on the new computer. You must initiate a new scan.

If one Symantec AntiVirus client in the cluster is unavailable temporarily, it receives the latest virus definitions when the Symantec AntiVirus service starts and the client checks in with the parent.

Logs and alerts include the name of the local computer but they do not include the cluster server name. This helps to identify which computer had the event.

Warning: Problems might occur if Symantec AntiVirus server or client is installed to a shared drive. For example, only one client and the shared drives will be protected. Also, manageability is lost after a failover.

About required restarts

When you run a silent installation on computers that are running Windows 98/ Me, a forced restart is required.

About email support

Symantec AntiVirus client can interface with supported email client software. This provides an additional level of antivirus protection that works in conjunction with Symantec server-side email protection products. It does not replace them.

The Symantec AntiVirus client installation program automatically detects installed Microsoft Exchange/Outlook and Lotus Notes clients and selects the appropriate option for installation. If you do not want to install the extra layer of protection provided by the email support, you can deselect each component during installation.

Note: If Lotus Notes is open when Symantec AntiVirus is installed, antivirus protection will not begin until Lotus Notes is restarted. Lotus Notes should be closed for five minutes after Symantec AntiVirus is installed and the Symantec AntiVirus service starts.

For users who regularly receive large attachments, you may want to disable Auto-Protect for email clients or not include the mail plug-in as part of the installation package. When Auto-Protect is enabled for email, attachments are immediately downloaded to the computer that is running the email client and scanned when the user opens the message. Over a slow connection with a large attachment, this slows mail performance.

Note: Symantec AntiVirus does not support the scanning of Exchange files or folders that are used on a Microsoft Exchange server. Scanning an Exchange directory can cause false positive virus detections, unexpected behavior on the Exchange server, or damage to the Exchange databases. If you install Symantec AntiVirus on a computer that is a Microsoft Exchange server, you should exclude the Microsoft Exchange directory structure from Auto-Protect scans.

For more information on excluding directories from Auto-Protect scans, see the *Symantec AntiVirus Administrator's Guide*. For more information on using Symantec AntiVirus products with Exchange servers, see the Symantec Knowledge Base.

About Internet email support

Symantec AntiVirus protects both incoming and outgoing email messages that use the POP3 or SMTP communications protocol. When Auto-Protect scanning for Internet email is enabled, Symantec AntiVirus scans both the body text of the email and any attachments that are included. If you do not want to install the extra layer of protection provided by Internet email support, you can deselect the Internet email scanning component during installation.

Note: If your network is configured to use non-standard ports for the POP3 or SMTP protocols, after you have installed Symantec AntiVirus you must configure the POP3 or SMTP ports that Symantec AntiVirus scans to match the ports that you are using for these protocols on your network.

For more information, see the *Symantec AntiVirus Administrator's Guide.*

Symantec AntiVirus also provides outbound email heuristics scanning, which uses Bloodhound Virus Detection to identify threats that may be contained in outgoing messages. Scanning outgoing email messages helps to prevent the spread of threats such as worms that can use email clients to replicate and distribute themselves across a network.

Email scanning does not support the following email clients:

- IMAP clients
- AOL clients

- POP3 that uses Secure Sockets Layer (SSL)
- HTTP-based email such as Hotmail and Yahoo!

Installation requirements

Symantec AntiVirus requires specific protocols, operating systems and service packs, software, and hardware.

All of the requirements that are listed for Symantec AntiVirus components are designed to work in conjunction with the hardware and software recommendations for the supported Microsoft Windows and NetWare computers. All computers to which you are installing Symantec AntiVirus should meet or exceed the recommended system requirements for the operating system that is used.

Review the following requirements before you install Symantec AntiVirus:

- Required protocols
- Symantec System Center and snap-in requirements
- Symantec AntiVirus server installation requirements
- Quarantine Server requirements
- Symantec AntiVirus client installation requirements

Required protocols

Symantec AntiVirus uses an adaptive communication method that handles IP and IPX communication. Benefits of this method are that Symantec AntiVirus does not require or create NetWare SAPs and it is compatible with IP-only networks.

Windows NT-based computers try to connect to NetWare servers first through IPX. If a NetWare server does not have IPX, then the Windows NT-based computer tries to connect with IP.

Specific combinations of mixed protocols can prevent proper communication. For example, if you are using the Symantec System Center to manage some computers running only IP and others running only IPX, you should have both protocols installed on the computer that is running the Symantec System Center.

You should avoid using the Symantec System Center console across a link that does not support the protocols that are used on the other side of the link. This also applies to setting up server groups that cross a link. For example, servers and clients will not be visible in the Symantec System Center if it is running on one side of an IP-only WAN link that is being used to connect NetWare servers that are running only IPX (no IP loaded) on the other side.

Note: If you are running Windows Me/XP, system disk space usage will be increased if you have the System Restore functionality enabled. For more information on how System Restore works, see the Microsoft Operating System documentation.

Symantec System Center and snap-in requirements

The Symantec System Center requires the following:

- Windows NT 4.0 Workstation/Server with Service Pack 6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Professional; Windows Server 2003 Web/Standard/Enterprise/Datacenter
- 32 MB RAM
- 36 MB disk space
- Internet Explorer 5.5 with Service Pack 2
- Microsoft Management Console version 1.2
  If MMC is not already installed, you will need 3 MB free disk space (10 MB during installation).

  Note: If Microsoft Management Console version 1.2 is not on the computer to which you are installing, the installation program will install it.

Quarantine Console requirements

The Quarantine Console must be installed on the Symantec System Center management console computer. The Quarantine Console has the following requirements:

- Windows NT 4.0 Workstation/Server with Service Pack 6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Professional
- 32 MB RAM
- 35 MB disk space (in addition to the Symantec System Center requirement)
- Internet Explorer 5.5 Service Pack 2
- Microsoft Management Console version 1.2
  If MMC is not already installed, you will need 3 MB free disk space (10 MB during installation).

Alert Management System snap-in requirements

The Alert Management System[2] snap-in requires 24 MB disk space in addition to the Symantec System Center requirements.

Symantec AntiVirus snap-in requirements

The Symantec AntiVirus snap-in requires 6 MB disk space in addition to the Symantec System Center requirements.

Symantec Client Firewall snap-in requirements

The Symantec Client Firewall snap-in requires 1 MB disk space in addition to the Symantec System Center requirements.

The Symantec Client Firewall snap-in is used for client firewall administration, which is not included with the Symantec AntiVirus product.

AV Server Rollout tool requirements

The AV Server Rollout tool requires 130 MB disk space in addition to the Symantec System Center requirements.

NT Client Install tool requirements

The NT Client Install tool requires 2 MB disk space in addition to the Symantec System Center requirements.

Symantec AntiVirus server installation requirements

Symantec AntiVirus server runs under several operating systems, each with unique installation requirements.

You should assign static IP addresses to Symantec AntiVirus servers. If a Symantec AntiVirus client is unavailable when its parent server's address changes, it will not be able to locate the parent server when it attempts to check in.

Microsoft Windows operating systems

Symantec AntiVirus server has the following Windows requirements:

- Windows NT 4.0 Workstation/Server/Terminal Server with Service Pack 6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Professional; Windows Server 2003 Web/Standard/Enterprise/Datacenter
- 64 MB RAM

- 111 MB disk space
- 15 MB disk space for AMS^2 server files (if you choose to install the AMS^2 server)
- Internet Explorer 4.01 or later
- Static IP address (recommended)

Note: Symantec AntiVirus does not support the scanning of Macintosh volumes on Windows servers for Macintosh viruses.

Novell NetWare operating systems

You should run the Novell client for NetWare on the computer from which Symantec AntiVirus will be rolled out to NetWare servers.

Symantec AntiVirus server has the following NetWare requirements:

- NetWare 5.1 with Support Pack 3 or higher; NetWare 6.0 with Support Pack 1 or higher; NetWare 6.5
- 15 MB RAM (above the standard NetWare RAM requirements) for Symantec AntiVirus NLMs
- 116 MB disk space (70 MB disk space for server files and 46 MB disk space for the client disk image)
- 20 MB disk space for AMS^2 server files (if you choose to install the AMS^2 server)

Note: Symantec AntiVirus is not supported on NetWare servers that are running SFT III.

Quarantine Server requirements

Quarantine Servers have the following requirements:

- Windows NT 4.0 Workstation/Server with Service Pack 6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Professional; Windows Server 2003 Web/Standard/Enterprise/Datacenter
- 64 MB RAM
- 40 MB disk space for Quarantine Server
- 500 MB to 4 GB disk space recommended for quarantined items

- Internet Explorer 5.5 with Service Pack 2
- Minimum swap file size of 250 MB

Note: If you are running Windows Me/XP, system disk space usage is increased if the System Restore functionality is enabled. For more information on how System Restore works, see the Microsoft operating system documentation.

Symantec AntiVirus client installation requirements

Symantec AntiVirus client requirements vary based on the type of protection installed to the computer. Disk space requirements are based on the installation of all features.

Symantec AntiVirus client for 32-bit computers

Symantec AntiVirus clients for 32-bit computers have the following requirements:

- Windows 98/98 SE/Me; Windows NT 4.0 Workstation/Server/Terminal Server with Service Pack 6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Home/Professional/Tablet PC; Windows Server 2003 Web/Standard/Enterprise/Datacenter
- 32 MB RAM minimum
- 55 MB disk space
- Root Certificate Update (Windows 98/98 SE)

Terminal Server clients connecting to a computer with antivirus protection have the following additional requirements:

- Microsoft Terminal Server RDP (Remote Desktop Protocol) client
- Citrix Metaframe (ICA) client 1.8 or later

Symantec AntiVirus client for 64-bit computers

Symantec AntiVirus clients for 64-bit computers have the following requirements:

- Windows XP 64-bit Edition Version 2003; Windows Server 2003 Enterprise/ Datacenter 64-bit
- 32 MB RAM minimum
- 70 MB disk space
- Internet Explorer 4.01 or later
- Itanium 2 processor

Requirements for legacy antivirus clients

Symantec AntiVirus supports antivirus protection on computers running the Windows 95 operating system with the Norton AntiVirus Corporate Edition 7.6 client.

For installation instructions, see the documentation that came with the software.

Requirements for clients that are running IPX only

When you install Symantec AntiVirus to computers that are running IPX only, the parent server to which they will connect must have Microsoft File and Print Services for NetWare installed. If you are installing from a network share on the parent server, or using a configurations file (Grc.dat) that contains the IPX address of the parent server, Microsoft File and Print Services for NetWare is not required on the server.

Chapter 4

Migrating to the current version of Symantec AntiVirus

This chapter includes the following topics:

Migration overview

Symantec AntiVirus provides a seamless upgrade from earlier versions of Symantec antivirus products, which helps to minimize risk and continually increase the quality of security tools available to administrators. The Symantec AntiVirus client and server installation programs use Microsoft Windows Installer (.msi) technology, which provides flexibility, a smaller deployment size, in-field patching, and a variety of deployment options for migrating from earlier versions of Symantec products to the current version.

Steps to migrating your network to the current version of Symantec AntiVirus

Upgrading to the current version of Symantec AntiVirus is a multi-step process. The steps should include the following:

- Create a migration plan.
  Before you begin rolling out the Symantec AntiVirus client, server, and administration upgrades, you should have a solid understanding of your network topology and a streamlined plan to maximize the protection of the resources on your network during the upgrade. Migrating your entire network to the current version (as opposed to managing multiple versions of Symantec AntiVirus) is strongly recommended.
  See "Creating migration plans" on page 78.
- Upgrade the Symantec System Center.
  Before you roll out new Symantec AntiVirus client or server installations, you should upgrade the Symantec System Center management snap-in. The Symantec System Center provides the rollout and management tools necessary to deploy the installation files, monitor installation status, and immediately manage the supported clients and servers that you are upgrading.
- Migrate the antivirus servers.
- Deploy Symantec AntiVirus to clients.

Supported and unsupported server and client migration paths

The following section lists the platforms that are supported and unsupported when migrating to the current version of Symantec AntiVirus.

If the migration of a program is supported, the Symantec AntiVirus setup program automatically detects the software, removes the legacy components and registry entries, and installs the new version. If the migration from a previous product is not supported, you must uninstall the program before you run the Symantec AntiVirus installation program.

In most cases, if you are migrating from a legacy antivirus program that is not included in the list of supported migration paths, the installation program will fail during the installation, the user is notified that the installation was unsuccessful, and the Windows Installer log is updated. However, in some cases, if you do not uninstall the unsupported product before you run the installation, the installation may appear to succeed, but the product may not function properly. You should always uninstall any antivirusprogram that is not included in the list of supported migration paths before attempting to install the current version.

Quit all other Windows programs before installing Symantec AntiVirus. Other active programs may interfere with the installation and reduce your protection.

After migrating from several of these supported platforms, the computers may need to be restarted before they will be protected by Symantec AntiVirus.

For the most up-to-date information on supported migration paths and potential migration issues, see the Symantec Knowledge Base.

Note: When migrating from Norton AntiVirus Corporate Edition version 7.6x to the current version of Symantec AntiVirus, you should migrate servers before you migrate clients. When clients are migrated first, but are connected to a parent server running 7.6x, the 7.6x client software attempts to install over the current client software.

Supported migration paths

Symantec AntiVirus can migrate seamlessly over the following products:

- Symantec AntiVirus Corporate Edition 8.0 and later
- Norton AntiVirus Corporate Edition 7.6 and later
- Symantec Client Security, all versions
- Norton Internet Security 2003 if the Norton AntiVirus component has not been installed

Unsupported migration paths

Symantec AntiVirus migration is not supported for the following products:

- Norton AntiVirus 2004 and earlier
- Norton Internet Security 2003 with Norton AntiVirus installed
- Norton Internet Security 2001/2002/2004
- Norton AntiVirus on NetWare platforms, all versions
- Norton AntiVirus for DOS/Windows 3.1, all versions
- Intel LANDesk Virus Protect, all versions
- IBM AntiVirus, all versions
- Norton AntiVirus as a part of Norton SystemWorks
- Antivirus products from other vendors

If Norton SystemWorks is detected when the Symantec AntiVirus setup program runs, Symantec AntiVirus will not install.

Unsupported migration of Administrator tools

Symantec AntiVirus migration is not supported for the following Administrator tools:

- Symantec System Center
- AMS^2 client and server
- LiveUpdate Administrator
- Quarantine Server and Quarantine Console

Custom settings may be lost

If you are not migrating from a supported migration path, any custom settings that you have are not saved during the migration process. On supported platforms, custom settings on clients and servers are preserved during migration.

Settings that are preserved for supported platforms include the following:

- Scheduled scans and LiveUpdate sessions
- All scan options
- All Auto-Protect options
- Custom exclusions and file extensions to scan
- LiveUpdate host files
- Symantec AntiVirus activity logs
- Quarantine forwarding information

Quarantine items are automatically migrated

If there are any items in Quarantine on Symantec AntiVirus clients or servers, they are migrated automatically to the Symantec AntiVirus Quarantine. However, if any items in Quarantine are determined by Symantec AntiVirus to be uninfected, they are deleted rather than migrated.

Creating migration plans

In general, upgrading from an earlier version of a Symantec AntiVirus product (such as Norton AntiVirus Corporate Edition 7.6) starts with the migration of the management console, followed by the migration of the servers, and ending with the migration of the clients. However, the actual sequence of events varies depending on your environment.

Evaluate the current system requirements

All computers on your network that are part of your migration plan should be evaluated with regard to the system requirements specified for the upgraded version of Symantec AntiVirus.

See “Installation requirements” on page 69.

Pilot your installation first

Do a small-scale installation to identify issues that are likely to occur in the larger migration. For instance, if a particular software configuration that is prevalent in your organization causes problems with the installation or operation of the client, the pilot should expose it. A good pilot candidate is the IS or support department. These departments usually have advanced users who will need to be familiar with the client at the start of the installation.

Minimize unprotected clients

If the migration entails the removal of existing antivirus software, there will be a short period of time when some clients are unprotected. You can minimize your exposure by staging the migration, and by trying to roll out as soon as possible after the previous antivirus software removal. Also, make sure that all of your servers, including GroupWare servers, are protected during this period. This will keep incidents isolated to a single computer.

Best Practice: Organize your clients into logical client groups to employ a multi-tiered rollout

When you are upgrading the clients and servers on your network to the current version of Symantec AntiVirus, you should organize your network into temporary groups that divide your network into logical deployment tiers. For example, you can create one group that is managed by a legacy Symantec AntiVirus Corporate Edition parent server and a second group that will be upgraded immediately to the current version. Once you have deployed the installations for the initial migrating group and tested that segment of your network, you can then upgrade the legacy group to bring your entire network up to the current version. If you organize your clients in this way, you can roll out installations incrementally, which helps to minimize the risk of a security breach.

Plan your virus definitions update strategy

Since there are several ways to update virus definitions files on clients and servers, you must decide which one to use before the installation, and test your update strategy during the pilot.

Decide how to handle remote and sometimes connected clients

When migrating from a version earlier than Norton AntiVirus Corporate Edition 7.x, your update mechanism and scheduled scans are not migrated automatically. You will need to reconfigure them when you install or update Symantec AntiVirus and the Symantec System Center.

Get virus definitions updating working immediately

You should set the update policy on migrated computers immediately after installation, and test it immediately after each stage of the installation.

Match management snap-in version to client version

You should always match the version of the management snap-in to the latest version of Symantec AntiVirus running on your clients. For example, to manage both Symantec AntiVirus 9.0 clients and supported legacy clients, use the latest version of the Symantec System Center console to which you have installed the 9.0 antivirus management snap-in. You cannot manage the latest client version with an older management snap-in.

Move servers among server groups

Although it is best to plan your server group structure before you begin the migration, you can move servers later. You can use a drag-and-drop operation in the Symantec System Center console to reorganize clients and servers.

Train your support staff and end users

You should designate some time to train end users and staff as a part of your installation plan. This minimizes downtime as a result of end-user confusion.

Server migration

There are several ways to install the Symantec AntiVirus server to supported Windows and NetWare operating systems, including third-party deployment options such as Active Directory. Uninstalling previously existing servers is generally not required prior to installation of Symantec AntiVirus server, provided that the server is not damaged.

See “Installing Symantec AntiVirus servers” on page 107.

About migrating from the Symantec System Center

Before you migrate the Symantec System Center, on the computer to which you are installing the Symantec System Center, you should uninstall the following:

- Any earlier versions of the Symantec System Center
- Any earlier versions of Symantec AntiVirus (including any versions of LANDesk Virus Protect)

The Symantec System Center can manage any earlier supported versions of Symantec AntiVirus, but the computer that is running the Symantec System Center must be using the current version of Symantec AntiVirus. You can install the Symantec System Center console to as many computers as you need to manage Symantec AntiVirus.

Manually uninstalling server components

The server components to uninstall depend on the version of the software currently installed, and on the operating system.

Norton AntiVirus Corporate Edition 7.5 or 7.6 on supported Windows and NetWare server operating systems

You can upgrade the server from Norton AntiVirus Corporate Edition 7.5 or 7.6 on supported Windows and NetWare server operating systems.

To prepare a server for an upgrade to the current version of Symantec AntiVirus

1. On the Windows desktop, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Add/Remove Programs**.
3. In the Add/Remove Programs dialog box, click **Symantec System Center**.
4. Click **Remove**.
5. Repeat steps 3 and 4 for the following components:
   - Norton AntiVirus Snap-in
   - Norton AntiVirus Add-On for the Symantec System Center console
   - Symantec Quarantine Console Snap-in
6. If desired, delete the contents of the Temp folder and the Recycle Bin.

7 Restart the computer.

8 Log on as the local administrator.

Symantec AntiVirus Corporate Edition 8.x on supported Windows and NetWare server operating systems

You can upgrade the server from Symantec AntiVirus Corporate Edition 8.0 and later on supported Windows and NetWare server operating systems.

To prepare a server for an upgrade to the current version of Symantec AntiVirus

1 On the Windows desktop, click **Start** > **Settings** > **Control Panel**.

2 In the Control Panel window, double-click **Add/Remove Programs**.

3 In the Add/Remove Programs dialog box, click **Symantec System Center**.

4 Click **Remove**.

5 Repeat steps 3 and 4 for the Symantec Quarantine Console Snap-in component.

6 If desired, delete the contents of the Temp folder and the Recycle Bin.

7 Restart the computer.

8 Log on as the local administrator.

Installing new server components

To migrate from an earlier version of Symantec AntiVirus, you must install the server and antivirus management components.

Installing the Symantec System Center console and components

You can install the Symantec System Center console and components from the Symantec AntiVirus CD.

To install the Symantec System Center console and components

1 From the Symantec AntiVirus CD, run Setup.exe.

2 On the Install Administrator Tools menu, click **Install Symantec System Center**.

3 In the welcome panel, click **Next**.

4 In the License Agreement panel, click **I accept the terms in the license agreement**, and then click **Next**.

5. In the Select Components panel, ensure that all items are selected, and then click **Next**.
6. In the Destination Folder panel, click **Next** for the default installation path.
7. In the Ready to Install the Program panel, click **Install**.
8. When the installation is complete, click **Finish**, and then restart the computer.

Installing the antivirus server program

You can install the antivirus server program from the Symantec AntiVirus CD.

To install Symantec AntiVirus server

1. From the Symantec AntiVirus CD, run Setup.exe.
2. In the Symantec AntiVirus panel, click **Install Symantec AntiVirus** > **Deploy AntiVirus Server**.
3. In the welcome panel, click **Update**, and then click **Next**.
4. Select the Computer Name, click **Add**, and then type the password for Server Group.
5. To proceed with the update, click **Finish**.
6. When the update process is finished, click **Close**, and then restart the computer.

Auto-Protect will start on the computer as soon as Symantec AntiVirus is installed, but the Alert Management System^2 (AMS^2) services will not start until after you restart the computer. If it is necessary to wait for a scheduled restart, the computer will be protected from the time of installation, but AMS^2 alerting will not work.

Note: Do not delete the NAV folder located by default at: <os drive>:\Program Files\NAV. A non-upgraded installation of Symantec AntiVirus server will create a folder called SAV located at \Program Files\SAV.

Installing the Central Quarantine Server

If you want to use the services of the Central Quarantine, you need to install the Central Quarantine Server.

To install the Central Quarantine Server

1. From the Symantec AntiVirus CD, run Setup.exe.
2. In the Symantec AntiVirus panel, click **Install Administrator Tools** > **Install Central Quarantine Server**.
3. In the welcome panel, click **Next**.
4. In the License Agreement panel, click **I agree**, and then click **Next**.
5. In the Destination Folder panel, click **Next** for the default installation path.
6. Click **Internet based (Recommended)**, and then click **Next**.
7. Specify the disk space, and then click **Next**.
8. Type contact information, and then click **Next**.
   Account Number is your Contact ID Number.
9. Do not make any changes to the default Gateway Name, and then click **Next**.
10. Click **Enable Alerts**, type the AMS Server Name (usually the primary server), and then click **Next**.
11. To install the Central Quarantine, click **Install**.
12. When the installation is complete, click **Finish**, and then restart the computer.

Installing the Quarantine Console

If you want to use the services of the Central Quarantine, you need to install the Quarantine Console.

To install the Quarantine Console

1. From the Symantec AntiVirus CD, run Setup.exe.
2. In the Symantec AntiVirus panel, click **Install Administrator Tools** > **Install Quarantine Console**.
3. In the welcome panel, click **Next**.
4. In the License Agreement panel, click **I agree**, and then click **Next**.
5. In the Destination Folder panel, click **Next** for the default installation path.

6 In the Ready to Install the Program panel, click **Install**.

7 When the installation is complete, click **Finish**.

Migrating from Symantec AntiVirus on NetWare platforms

The Symantec AntiVirus installation program detects earlier supported versions of Symantec AntiVirus on NetWare platforms. However, if you are migrating from a version that is not supported, you must manually uninstall Symantec AntiVirus on NetWare platforms from the servers to be migrated.

Migrate from supported and unsupported versions of Symantec AntiVirus on NetWare platforms

You can migrate from supported and unsupported versions of Symantec AntiVirus on NetWare platforms.

To migrate from a supported version of Symantec AntiVirus on NetWare platforms

1 From the Symantec AntiVirus CD, run Setup.exe.

2 In the Symantec AntiVirus panel, click **Install Symantec AntiVirus** > **Deploy AntiVirus Server**.

3 In the welcome panel, click **Update**, and then click **Next**.

4 In the Select Computers panel, select the Computer Name, click **Add**, and then type the password for Server Group.

5 Click **Finish** to proceed with the update.

6 When the update process is finished, click **Close**, and then restart the computer.

To migrate from an unsupported version of Symantec AntiVirus on NetWare platforms

1 On the servers that you want to migrate that run Symantec AntiVirus on NetWare platforms, unload Symantec AntiVirus from the Symantec AntiVirus console on the server.
If you do not unload the Symantec AntiVirus NLM and you try to install the current version of Symantec AntiVirus, the installation will fail when you try to load Vpstart /Install.

2 Remove the Symantec AntiVirus files from the server.

3 Use the NetWare Administrator (Nwadmin32.exe or Nwadmn95.exe) to remove the Symantec AntiVirus server object from the NDS tree.

4 Remove the Symantec AntiVirus load line from Autoexec.ncf, if necessary.

5. From the Symantec AntiVirus CD, run Setup.exe to install Symantec AntiVirus to your NetWare server.
6. When prompted to select Install or Update, click **Install**.
7. Select the server groups for the NetWare servers.
   You can move the servers between server groups later.
   All settings from the earlier version of Symantec AntiVirus are lost and must be reset in the Symantec System Center console after Symantec AntiVirus is installed.

You can uninstall the Symantec AntiVirus client console program at your convenience by running its uninstallation item from the Symantec AntiVirus program group on the client computer.

About migration from other server antivirus products

The Symantec AntiVirus installation requires all products that are not automatically uninstalled to be removed from the servers prior to installation.

Symantec AntiVirus also includes the Security Software Uninstaller that can detect and remove versions of antivirus software that are not included in the list of supported migration paths. For more information on using the Security Software Uninstaller, see the documentation provided for the tool in the \Tools\UNINSTLL directory on the Symantec AntiVirus CD.

After the antivirus program is uninstalled, the servers are treated like any other servers to which Symantec AntiVirus is rolled out.

Client migration

There are several ways to install the Symantec AntiVirus client to supported Windows operating systems, including third-party deployment options such as Active Directory. Uninstalling previously existing clients is generally not required prior to installation of Symantec AntiVirus client, provided that the client is not damaged.

See “Installing Symantec AntiVirus clients” on page 129.

Installing from the CD

To migrate from an earlier version of Symantec AntiVirus, you can follow the standard installation procedure for installing a client.

See “Installing Symantec AntiVirus clients locally” on page 150.

To install a client upgrade from the CD

1. From the Symantec AntiVirus CD, run Setup.exe.
2. In the Symantec AntiVirus panel, click **Install Symantec AntiVirus** > **Install AntiVirus Client**.
3. Proceed with the upgrade process.
4. Restart the computer.

Installing from the Symantec System Center

To migrate from an earlier version of Symantec AntiVirus, you can deploy a client installation from the Symantec System Center.

To install a client upgrade from the Symantec System Center

1. In the Symantec System Center, in the left pane, click **System Hierarchy** or any object under it.
2. On the Tools menu, click **NT Client Install**.
   NT Client Install is available only if the NT Client Install tool was selected when you installed the Symantec System Center. This component is selected for installation by default.
3. Continue the installation.
   See "Running the client setup program" on page 134.

How to determine parent servers and policy

When Symantec AntiVirus is installed to servers, each server receives a full set of installation files for all supported platforms in the folder Program Files\Sav\Clt-inst on a Windows NT-based server and SYS:SAV\clt-inst on a NetWare server.

Note: If you have servers running Symantec AntiVirus that you know will never serve as parents, you can remove the \Clt-inst directory and its sub-directories to reclaim approximately 50 MB of hard disk space.

When the antivirus policy is set on the server, the policy settings are saved in the Grc.dat file. This file exists in all of the installation sets and is updated any time that the policy is changed. When Symantec AntiVirus is then installed to clients from these installation sets, the policy is carried to the clients with this file, along with the identification of the parent server.

When clients are migrated from earlier versions of Symantec AntiVirus, the folder to which that version is installed is used.

Note: When migrating to the current version of Symantec AntiVirus, migrate servers before you migrate clients.

Windows NT/2000/XP/2003 client migrations

There are several recommended methods for migrating Windows NT-based clients, as follows:

- Use a logon script. If this method is used, the users will need to have local administrator rights to the Windows computer with which they are logging on.
- Use the NT Client Install tool. The NT Client Install tool removes the necessity of users having local administrator rights and logging on. The administrator running the NT Client Install tool must have administrator rights to the domain to which the client computers belong. You can run the NT Client Install tool from the Symantec System Center console. Use the Tools menu and click NT Client Install or run Ntremote.exe directly from the \Rollout\NTClient folder on the Symantec AntiVirus CD.
- Have users execute Setup.exe (or Setup.exe /s /v/qn for a silent installation) directly from the Vphome\Clt-inst\Win32 folder on their assigned parent server. If this method is used, the users need to have local administrator rights to the computer to which they are installing.

In each case, automatic migration from earlier versions of Symantec AntiVirus occurs. Also, the clients inherit the policy that was set on the parent server.

See “Client installation methods” on page 130.

Note: If the Symantec AntiVirus user interface (Vpc32.exe) is open when you try to install Symantec AntiVirus, the migration and installation stop on the client.

Windows 98/Me client migrations

There are two recommended methods for migrating Windows 98/Me clients:

- Use a logon script.
- Have users execute Setup.exe (or Setup.exe /s /v/qn for a silent installation) directly from the Vphome\Clt-inst\Win32 folder on their destined parent server.

In each case, automatic migration from earlier versions of Symantec AntiVirus occurs. Also, the clients inherit the policy that was set on the parent server immediately.

During the migration of Windows 98/98 SE clients, the installation program requires the user to click OK when prompted to restart the computer.

See “Client installation methods” on page 130.

Note: If the Symantec AntiVirus user interface (Vpc32.exe) is open when you try to install Symantec AntiVirus, the migration and installation stop on the client.

Other antivirus product client migrations

Since the Symantec AntiVirus installation will not recognize the presence of other antivirus products, the products must be removed prior to the rollout.

Symantec AntiVirus includes the Security Software Uninstaller that can detect and remove versions of antivirus software that are not included in the list of supported migration paths. For more information on using the Security Software Uninstaller, see the documentation provided for the tool in the \Tools\UNINSTLL directory on the Symantec AntiVirus CD.

Existing LiveUpdate server migration

If you have already set up LiveUpdate FTP servers or UNC paths, there is no need to modify them. They will continue to be used the same way with Symantec AntiVirus.

When the Symantec System Center is installed, you have the option to install LiveUpdate Administrator as well. To continue to use an internal LiveUpdate server, install LiveUpdate Administrator to at least one of your supported Windows servers. This lets you schedule LiveUpdate Administration Utility retrieval of packages directly from the Symantec System Center.

Installing Symantec AntiVirus management components

This chapter includes the following topics:

Installing the Symantec System Center

The Symantec System Center is installed directly from the Symantec AntiVirus CD. Install the Symantec System Center to the computers from which you want to manage your antivirus protection.

In addition to the Symantec System Center, the following management components are installed by default:

- Alert Management System^2 (AMS^2) console: Required if you want to use the enhanced alerting that is provided by AMS^2.
- Symantec AntiVirus snap-in: Required if you want to centrally manage antivirus protection.
- Symantec Client Firewall snap-in: Required if you want to centrally distribute firewall policy files.

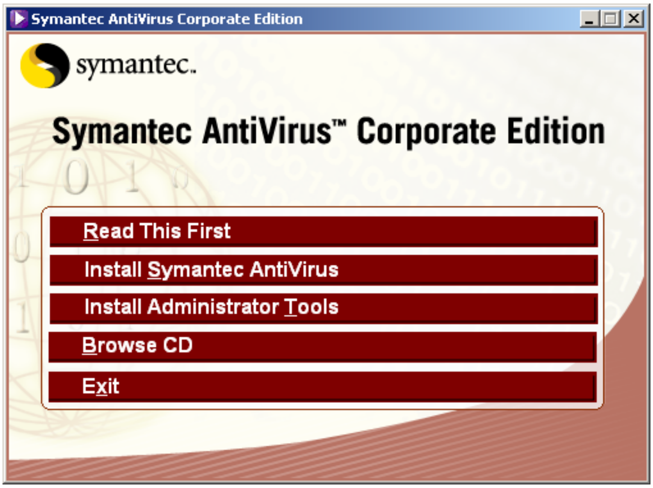
- AV Server Rollout tool: Adds the ability to push the server installation to remote computers. This tool is also available on the Symantec AntiVirus CD.
- NT Client Install tool: Adds the ability to push the Symantec AntiVirus client installation to remote computers running supported Microsoft Windows operating systems. This tool is also available on the Symantec AntiVirus CD.

If you elect not to install any of these management components with the Symantec System Center, you can run the Symantec System Center installation later and select them.

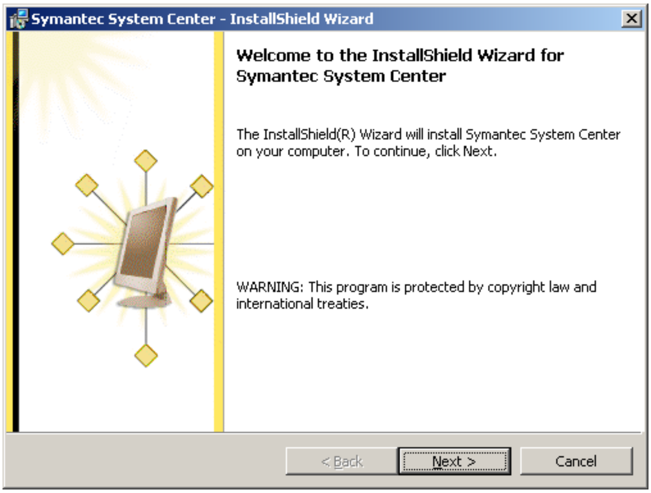
Note: If you are not managing Symantec Client Firewall clients, you do not need to install the Symantec Client Firewall snap-in. However, doing so will not cause any problems. Symantec Client Firewall is not included with Symantec AntiVirus.

To install the Symantec System Center

1 Insert the Symantec AntiVirus CD into the CD-ROM drive.


Symantec AntiVirus Corporate Edition
symantec.
Symantec AntiVirus™ Corporate Edition
Read This First
Install Symantec AntiVirus
Install Administrator Tools
Browse CD
Exit

2 In the Symantec AntiVirus panel, click **Install Administrator Tools** > **Install Symantec System Center**.

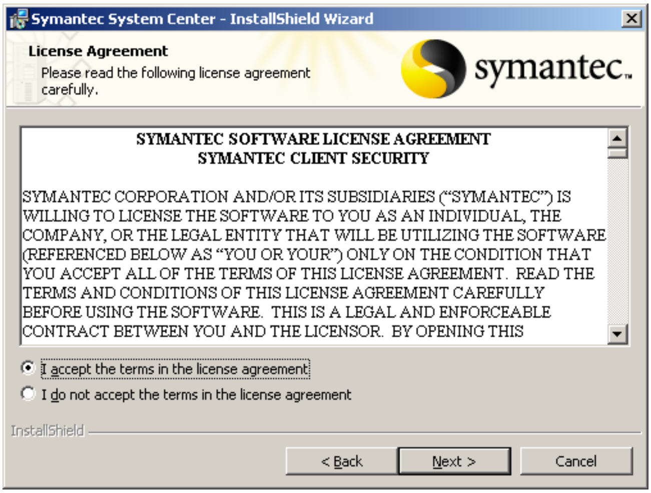

Symantec System Center - InstallShield Wizard

Welcome to the InstallShield Wizard for Symantec System Center

The InstallShield(R) Wizard will install Symantec System Center on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

3 In the welcome panel, click **Next**.


Symantec System Center - InstallShield Wizard

License Agreement

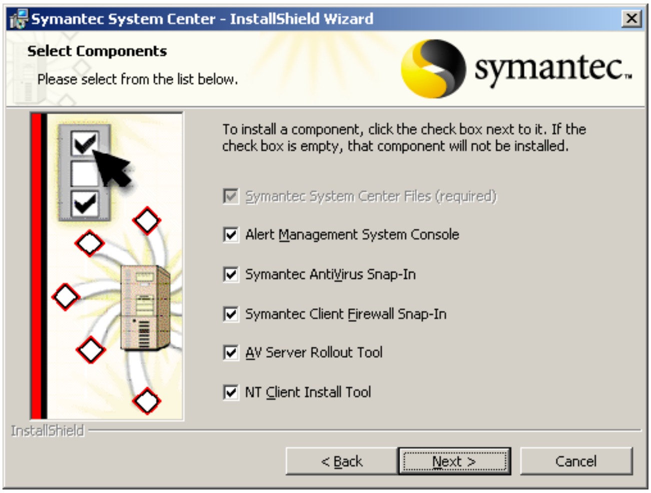
Please read the following license agreement carefully.

SYMANTEC SOFTWARE LICENSE AGREEMENT
SYMANTEC CLIENT SECURITY

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES (“SYMANTEC”) IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS “YOU OR YOUR”) ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS

● I accept the terms in the license agreement
○ I do not accept the terms in the license agreement

4 In the License Agreement panel, click **I accept the terms in the license agreement**, and then click **Next**.



Symantec System Center - InstallShield Wizard

Select Components

Please select from the list below.

To install a component, click the check box next to it. If the check box is empty, that component will not be installed.

☑ Symantec System Center Files (required)

☑ Alert Management System Console

☑ Symantec AntiVirus Snap-In

☑ Symantec Client Firewall Snap-In

☑ AV Server Rollout Tool

☑ NT Client Install Tool

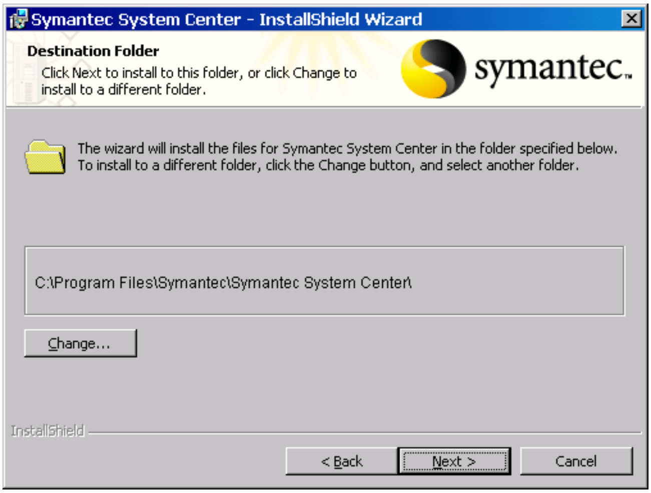
If Microsoft Management Console version 1.2 is not installed on the computer, a message indicates that you must allow it to install.

5 In the Select Components panel, check any of the following components that you want to install:

- Alert Management System Console
- Symantec AntiVirus Snap-In
- Symantec Client Firewall Snap-In
- AV Server Rollout Tool
- NT Client Install Tool

If these components are not present on the computer, all of them will be checked automatically.

6 Click **Next**.



Symantec System Center - InstallShield Wizard

Destination Folder

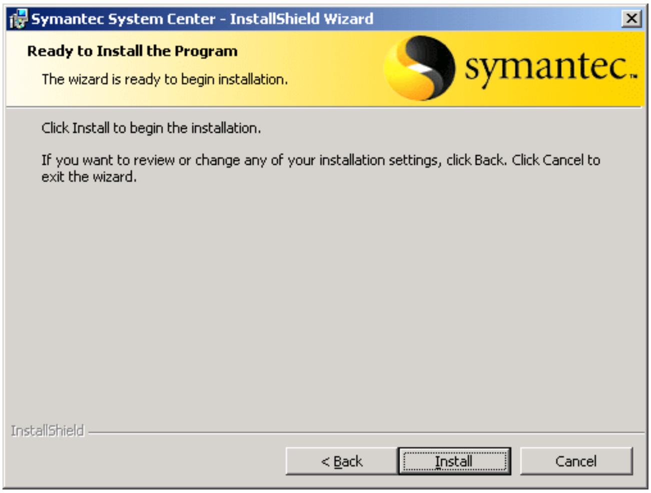
Click Next to install to this folder, or click Change to install to a different folder.

The wizard will install the files for Symantec System Center in the folder specified below. To install to a different folder, click the Change button, and select another folder.

C:\Program Files\Symantec\Symantec System Center\

7 In the Destination Folder panel, do one of the following:

- To accept the default destination folder, click **Next**.
- Click **Change**, locate and select a destination folder, click **OK**, and then click **Next**.



Symantec System Center - InstallShield Wizard

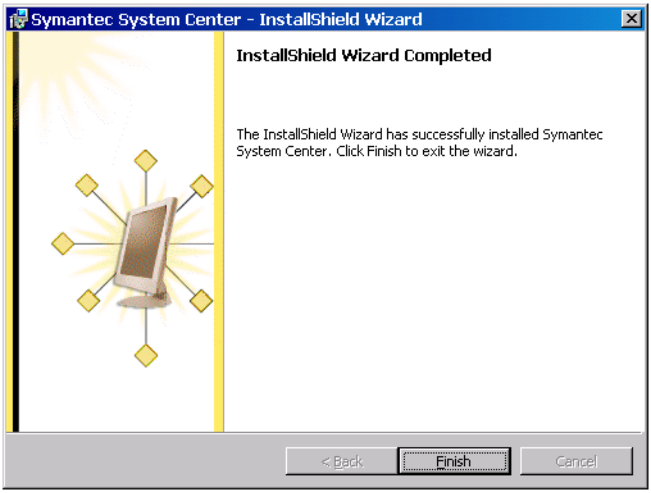
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

8 In the Ready to Install the Program panel, click **Install**.



Symantec System Center - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Symantec System Center. Click Finish to exit the wizard.

You may be prompted to restart the computer if the Microsoft Management Console is installed.

9 In the InstallShield Wizard Completed panel, to close the wizard, click **Finish**.

10 When you are prompted to restart the computer, select one of the following:

- Yes
- No

The computer must be restarted before you can do either of the following:

- Install Central Quarantine.
- Use the AMS^2 console.

If you want to install other components first, you can skip the restart.

11 Click **Finish**.

Installing the Central Quarantine

The Central Quarantine is composed of the Quarantine Server and the Quarantine Console. The Quarantine Server and the Quarantine Console can be installed on the same or different supported Windows computers.

The Quarantine Server is managed by the Quarantine Console, which snaps in to the Symantec System Center. To manage the Central Quarantine from the Symantec System Center console, the Quarantine Console snap-in must be installed.

Installation of the Central Quarantine requires the following tasks:

- Install the Quarantine Console snap-in.
- Install the Quarantine Server.

When you complete the installation, you can configure the Central Quarantine.

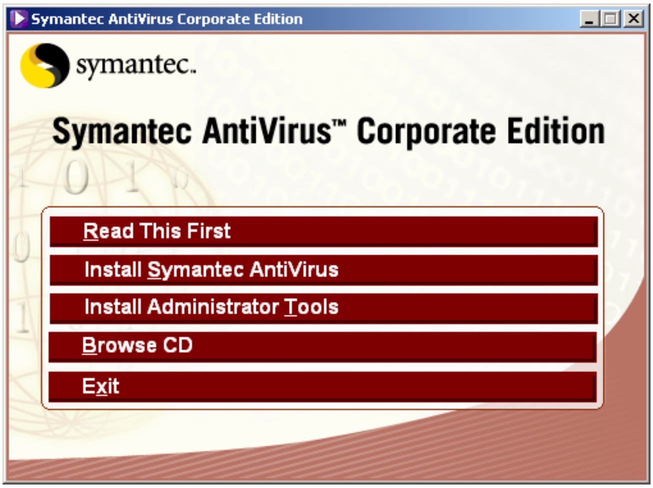
For more information, see the *Symantec Central Quarantine Administrator's Guide* on the Symantec AntiVirus CD.

Install the Central Quarantine

You must install both the Quarantine Console snap-in and the Quarantine Server.

To install the Quarantine Console snap-in

1 On the computer on which the Symantec System Center is installed, insert the Symantec AntiVirus CD into the CD-ROM drive.


Symantec AntiVirus Corporate Edition
symantec.
Symantec AntiVirus™ Corporate Edition
Read This First
Install Symantec AntiVirus
Install Administrator Tools
Browse CD
Exit

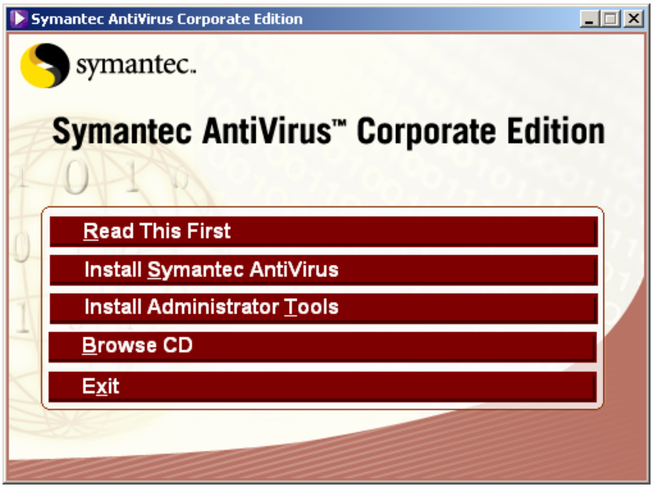
If your computer is not set to automatically run a CD, you must manually run Setup.exe.

2 In the Symantec AntiVirus panel, click **Install Administrator Tools** > **Install Quarantine Console**.

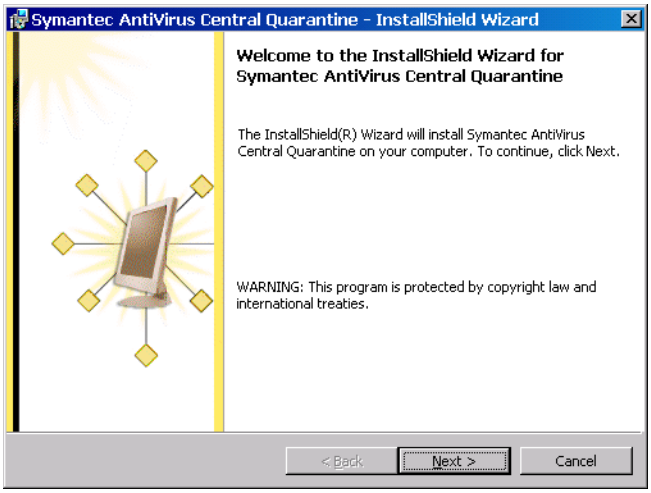
3 Follow the on-screen instructions.

To install the Quarantine Server

1 On the computer on which you want to install the Quarantine Server, insert the Symantec AntiVirus CD into the CD-ROM drive.


Symantec AntiVirus Corporate Edition
symantec.
Symantec AntiVirus™ Corporate Edition
Read This First
Install Symantec AntiVirus
Install Administrator Tools
Browse CD
Exit

2 In the Symantec AntiVirus panel, click **Install Administrator Tools** > **Install Central Quarantine**.

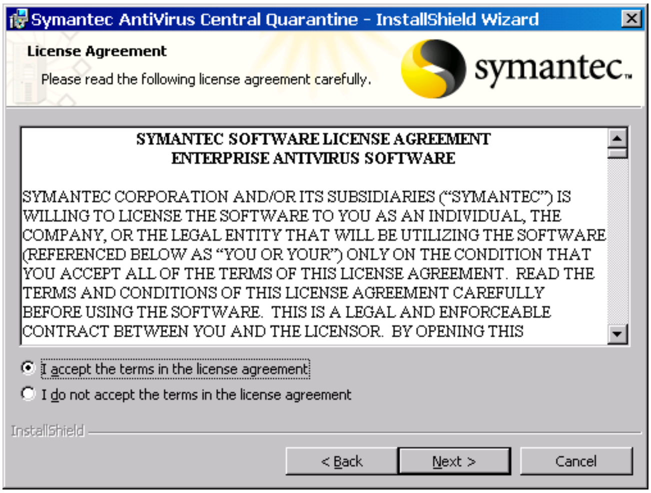

Symantec AntiVirus Central Quarantine - InstallShield Wizard
< Back
Next >
Cancel

Welcome to the InstallShield Wizard for Symantec AntiVirus Central Quarantine

The InstallShield(R) Wizard will install Symantec AntiVirus Central Quarantine on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

3 In the welcome panel, click **Next**.



Symantec AntiVirus Central Quarantine - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

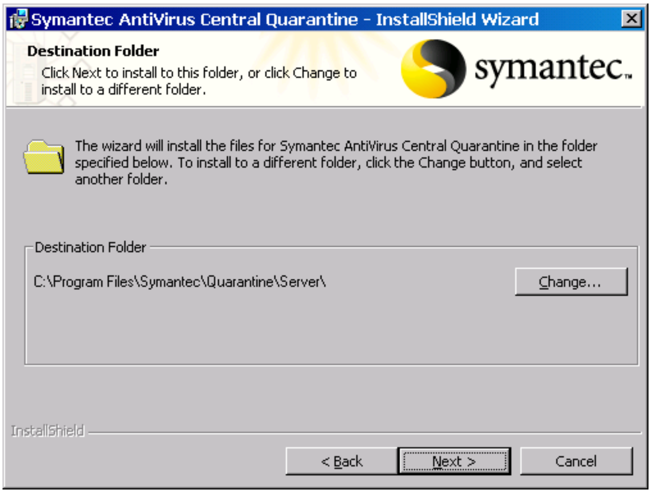
SYMANTEC SOFTWARE LICENSE AGREEMENT
ENTERPRISE ANTIVIRUS SOFTWARE

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

4 In the License Agreement panel, click **I accept the terms in the license agreement**, and then click **Next**.



Symantec AntiVirus Central Quarantine - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

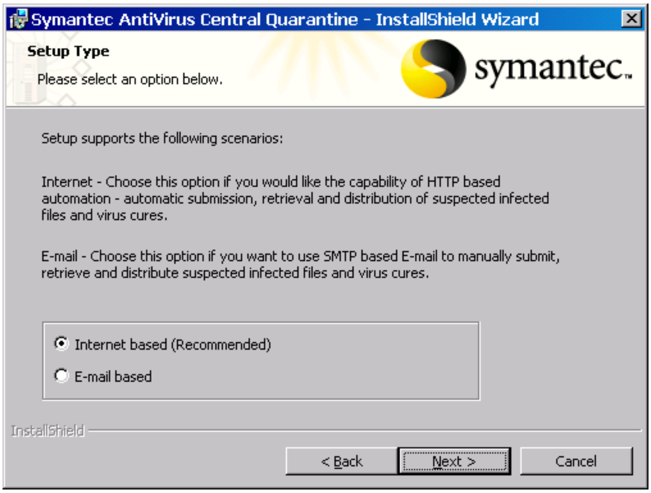
The wizard will install the files for Symantec AntiVirus Central Quarantine in the folder specified below. To install to a different folder, click the Change button, and select another folder.

Destination Folder

C:\Program Files\Symantec\Quarantine\Server\

5 In the Destination Folder panel, do one of the following:

- To accept the default destination folder, click **Next**.
- Click **Change**, locate and select a destination folder, click **OK**, and then click **Next**.


Symantec AntiVirus Central Quarantine - InstallShield Wizard
symantec.
InstallShield
< Back
Next >
Cancel

Setup Type

Please select an option below.

Setup supports the following scenarios:

Internet - Choose this option if you would like the capability of HTTP based automation - automatic submission, retrieval and distribution of suspected infected files and virus cures.

E-mail - Choose this option if you want to use SMTP based E-mail to manually submit, retrieve and distribute suspected infected files and virus cures.

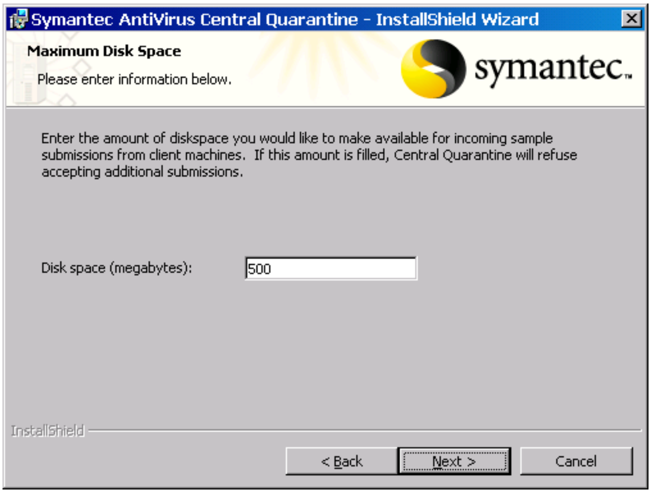
● Internet based (Recommended)

○ E-mail based

6 In the Setup Type panel, select one of the following:

- Internet based (Recommended)
- E-mail based

7 Click **Next**.


Symantec AntiVirus Central Quarantine - InstallShield Wizard
symantec.
InstallShield
< Back
Next >
Cancel

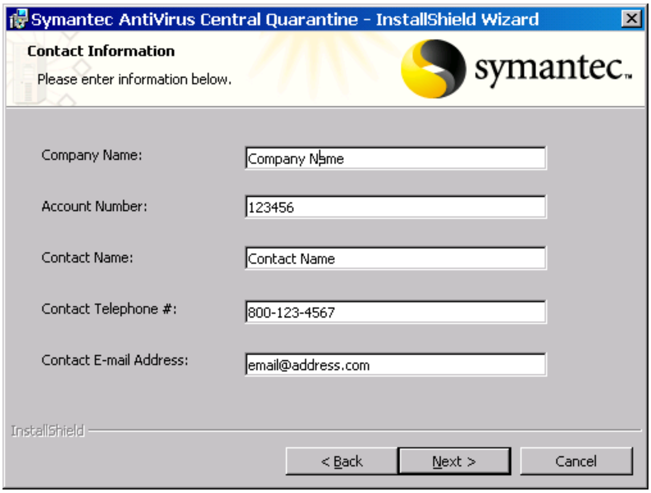
Maximum Disk Space

Please enter information below.

Enter the amount of diskspace you would like to make available for incoming sample submissions from client machines. If this amount is filled, Central Quarantine will refuse accepting additional submissions.

Disk space (megabytes): 500

8 In the Maximum Disk Space panel, type the amount of disk space to make available on the server for Central Quarantine submissions from clients, and then click **Next**.



Symantec AntiVirus Central Quarantine - InstallShield Wizard

Contact Information

Please enter information below.

Company Name: Company Name

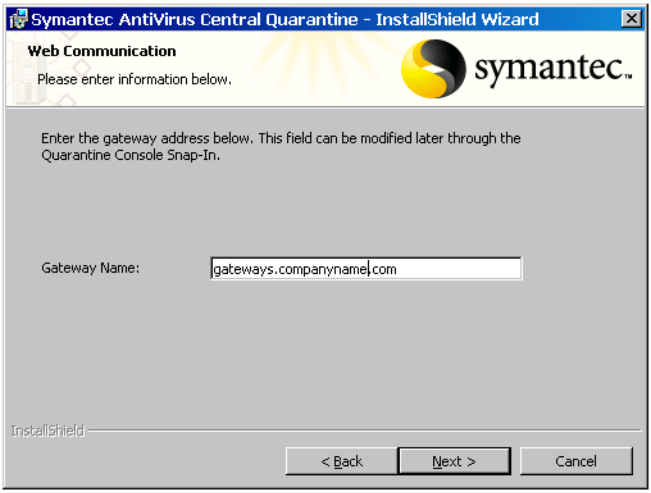
Account Number: 123456

Contact Name: Contact Name

Contact Telephone #: 800-123-4567

Contact E-mail Address: email@address.com

9 In the Contact Information panel, type your company name, your Symantec contact ID/account number, and contact information, and then click **Next**.



Symantec AntiVirus Central Quarantine - InstallShield Wizard

Web Communication

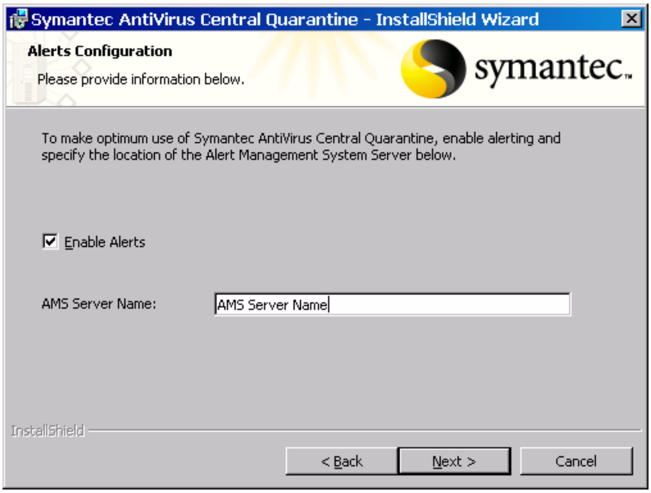
Please enter information below.

Enter the gateway address below. This field can be modified later through the Quarantine Console Snap-In.

Gateway Name: gateways.companyname.com

10 In the Web Communication panel, change the gateway address if necessary, and then click **Next**.

By default, the Gateway Name field is filled in with the gateway address.


Symantec AntiVirus Central Quarantine - InstallShield Wizard
symantec.
InstallShield
< Back
Next >
Cancel

Alerts Configuration

Please provide information below.

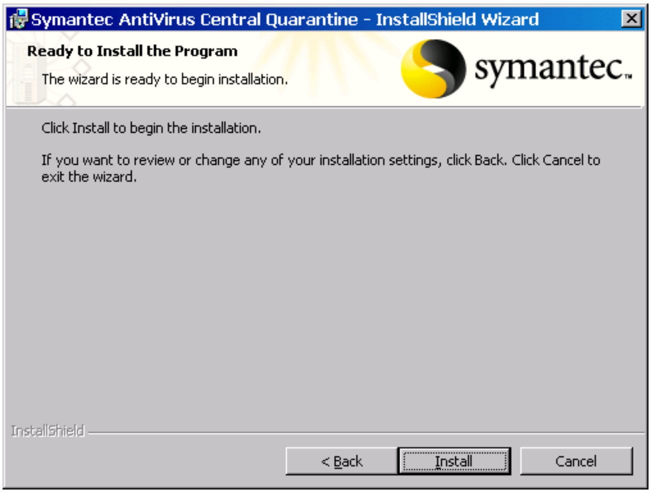
To make optimum use of Symantec AntiVirus Central Quarantine, enable alerting and specify the location of the Alert Management System Server below.

☑ Enable Alerts

AMS Server Name: AMS Server Name

11 In the Alerts Configuration panel, check **Enable Alerts** to use AMS^2, type the name of your AMS^2 server, and then click **Next**.

You can leave this blank if no AMS^2 server is installed.


Symantec AntiVirus Central Quarantine - InstallShield Wizard
symantec.
InstallShield
< Back
Install
Cancel

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

12 In the Ready to Install the Program panel, click **Install**, and then follow the on-screen prompts to complete the installation.

13 Write down the IP address or host name of the computer on which you installed the Quarantine Server.
This information will be required when you configure client programs to forward items to the Central Quarantine.

Installing and configuring the LiveUpdate Administration Utility

You can use the LiveUpdate Administration Utility to create a single download point for virus definitions and updates to Symantec products that use LiveUpdate. You can set up a LiveUpdate server on one or more Internet-ready computers to distribute updates across an internal local area network (LAN).

For more information, see the *LiveUpdate Administrator's Guide* on the Symantec AntiVirus CD.

To set up a LiveUpdate server with the LiveUpdate Administration Utility, and to set up servers to retrieve updates from the LiveUpdate server, complete the following tasks:

- Install the LiveUpdate Administration Utility.
  Configure the LiveUpdate Administration Utility scheduling from the Symantec System Center console to download updates from Symantec.
- Configure the LiveUpdate Administration Utility.
  Specify the packages to download and the directory to which the packages will be downloaded.
  If you have workstations that are connected to a UNC network location, the user who is logged on to the network must have access rights to the network resource. The user name and password that are supplied in the host file are ignored. With a Windows NT server, you can create a shared resource that all users are authorized to access (a NULL share). For more information on creating a NULL share, see the Microsoft Windows NT server documentation.
- Ensure that your FTP server, Web server, or UNC share is configured to share files from the download directory that you specified.

- In the Symantec System Center console, do the following:
  - Configure LiveUpdate for the internal LiveUpdate server.
  - Configure other servers and clients to download virus definitions and program updates from the internal LiveUpdate server.
  - Schedule when you want LiveUpdate sessions to run.

Many administrators prefer to test virus definitions files on a test network before making them available on a production server. If you test your virus definitions files, test them on your test network. Once testing is complete, run LiveUpdate from your production network.

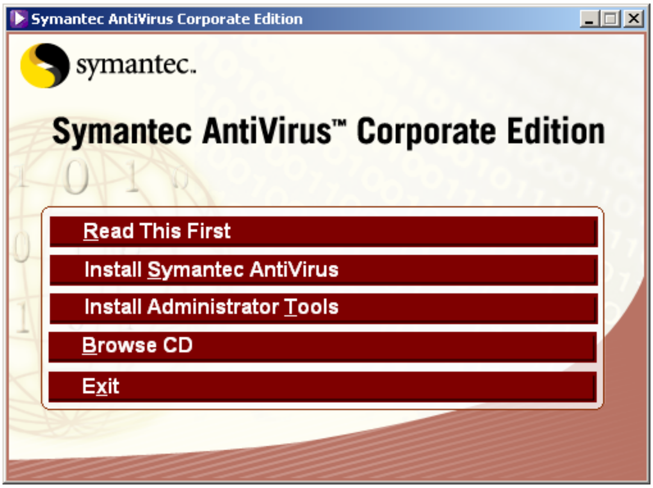
Install and configure the LiveUpdate Administration Utility

Install the LiveUpdate Administration Utility on a Windows NT computer that is running the server program, and then configure it.

For more information on using the LiveUpdate Administration Utility, see the *LiveUpdate Administrator's Guide* PDF on the Symantec AntiVirus CD.

To install the LiveUpdate Administration Utility

1 Insert the Symantec AntiVirus CD into the CD-ROM drive.


Symantec AntiVirus Corporate Edition
symantec.
Symantec AntiVirus™ Corporate Edition
Read This First
Install Symantec AntiVirus
Install Administrator Tools
Browse CD
Exit

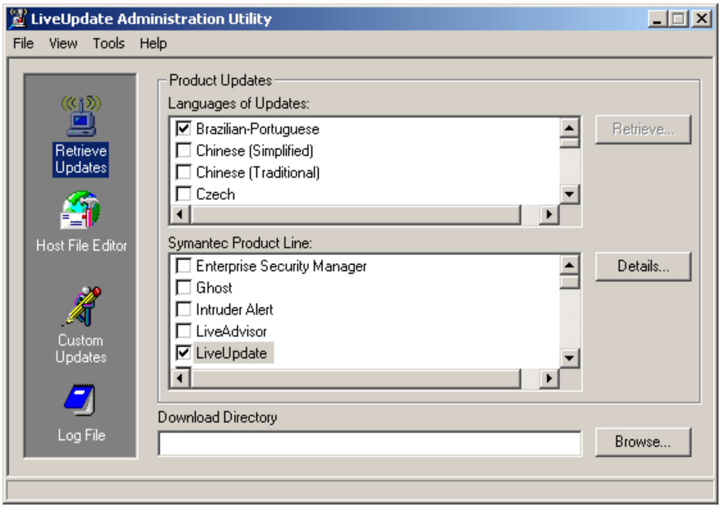
2 In the Symantec AntiVirus panel, click **Install Administrator Tools** > **Install LiveUpdate Administrator**.

3 Follow the on-screen instructions.

To configure the LiveUpdate Administration Utility

1 On the Windows taskbar, click **Start** > **Programs** > **LiveUpdate Administration Utility** > **LiveUpdate Administration Utility**.

2 Click **Retrieve Updates**.



Languages of Updates:

- ☑ Brazilian-Portuguese
- □ Chinese (Simplified)
- □ Chinese (Traditional)
- □ Czech

Symantec Product Line:

- □ Enterprise Security Manager
- □ Ghost
- □ Intruder Alert
- □ LiveAdvisor
- ☑ LiveUpdate

Download Directory

3 In the LiveUpdate Administration Utility window, under Download Directory, type or select the download directory on your LiveUpdate server.

This is the location in which the update packages and virus definitions files will be stored once they are downloaded from Symantec. (Files are downloaded to a temporary directory that is created by the LiveUpdate Administration Utility. Once the file is downloaded, it is moved to the specified Download Directory.) The Download Directory can be any directory on your server.

4 Under Languages of Updates, select the language for downloaded packages.

5 Under Symantec Product Line, check the Symantec product lines for which you want to receive packages.

You can select individual product components to update, but you risk missing other available updates. For example, new virus definitions files for Symantec AntiVirus might require an engine update that is also available for download.

Because all installed Symantec products that use LiveUpdate now point to your intranet server, it is safer to download full product lines rather than individual products.

Where to find Symantec VPN Sentry installation instructions

Vendor-specific Symantec VPN Sentry installation packages and documentation are located on the Symantec AntiVirus CD in the SymSentry folder.

Uninstalling Symantec AntiVirus management components

You can uninstall all of the Symantec AntiVirus management components using Add/Remove Programs in the Control Panel on the local computer. You can also uninstall only the Symantec System Center.

Uninstalling the Symantec System Center

When you uninstall the Symantec System Center, all of its components, including snap-ins, are also uninstalled.

Uninstall the Symantec System Center

You can uninstall the Symantec System Center using the Windows Add/Remove Programs option.

To uninstall the Symantec System Center from Windows NT Server/ Workstation

1. On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Add/Remove Programs**.
3. In the Add/Remove Programs dialog box, click **Symantec System Center**.
4. Click **Add/Remove**.
5. Click **Yes** to confirm.

To uninstall the Symantec System Center from Windows 2000 Professional/ Server/Advanced Server/XP

1. On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Add/Remove Programs**.
3. In the Add/Remove Programs dialog box, click **Symantec System Center**.
4. Click **Change/Remove**.
5. When the uninstallation completes, click **Close**.

Chapter 6

Installing Symantec AntiVirus servers

This chapter includes the following topics:

Server installation methods

You can install Symantec AntiVirus servers using any of the methods that are listed in Table 6-1. You can use any combination of methods that suits your network environment.

Table 6-1 Server installation methods

Method	Description	Preparation
Push	You can push a Symantec AntiVirus server installation directly from the Symantec AntiVirus CD or from the Symantec System Center. See “Deploying the server installation across a network connection” on page 112.	Install the Symantec System Center with the antivirus management snap-in and the AV Server Rollout tool to push the server installation from the Symantec System Center.

Table 6-1 Server installation methods

Method	Description	Preparation
Windows Installer (.msi) deployment	You can customize and deploy an installation package using tools that are compatible with Windows Installer. Symantec AntiVirus uses Windows Installer technology for all client and server installations. Symantec AntiVirus uses the standard Windows Installer deployment options provided by Microsoft. The only prerequisite is that you are familiar with Windows Installer package creation and deployment.	Create a custom .msi installation using the components and options specific to Symantec AntiVirus installation packages. See "Windows Installer (.msi) command-line reference" on page 161.
Symantec Packager self-extracting executable	You can create a package with Symantec Packager that includes a preconfigured Windows Installer package or set of packages. Distribute and execute a package to install Symantec AntiVirus server directly onto a computer. Customizing the Windows Installer installation packages using Symantec Packager is not supported. **Note:** Symantec Packager is included with this release of Symantec AntiVirus as an unsupported tool. For more information, see *Using Symantec Packager with Symantec AntiVirus* (pkgrinfo.pdf) in the Symantec Packager folder on the Symantec AntiVirus CD.	■ Create a custom Symantec AntiVirus server Windows Installer package, if desired. ■ Determine a method for distributing and executing the package.

About Symantec AntiVirus server installation

The Symantec AntiVirus server program does the following:

- Protects the computer on which it is running
- Manages other Symantec AntiVirus servers and clients

  If a Windows-based network server needs protection only, install the Symantec AntiVirus client program.

  See "Installation requirements" on page 69.

You can install the Symantec AntiVirus server program using any of the following methods:

- Deploy the server installation across a network connection to remote computers from the Symantec System Center or the Symantec AntiVirus CD. The Symantec AntiVirus server installation program installs AMS^2 by default to all computers to which you've installed Symantec AntiVirus server.
  See "Why AMS is installed with Symantec AntiVirus server" on page 109.
  See "Deploying the server installation across a network connection" on page 112.
- Create a customized Windows Installer (.msi) package using the standard Windows Installer options and the Symantec-specific options that are provided.
  See "Windows Installer (.msi) command-line reference" on page 161.

Why AMS is installed with Symantec AntiVirus server

If you plan to use AMS^2 to generate alerts based on antivirus events, you must install AMS^2 to every primary server. When you install Symantec AntiVirus server to supported Windows and NetWare computers, AMS^2 is selected for installation by default.

While AMS^2 is required to run only on the primary server, you should install AMS^2 to all of the computers on which you install the Symantec AntiVirus server program. This lets you change primary servers without reinstalling AMS^2 on the new primary server. If a secondary server needs to be made a primary server, no AMS^2 events will be lost.

In the Symantec System Center, you can select the computer that will perform many AMS^2 actions. AMS^2 is required for some of the actions to run. Installing AMS^2 on more computers gives you flexibility in choosing the computers that can perform advanced alert actions, such as sending pages.

If you do not install AMS^2 when you install Symantec AntiVirus server, you can install it later. You must, however, install AMS^2 to the secondary server before making the secondary server the primary server.

See "Manually installing AMS server" on page 126.

If you do not plan to change your primary servers, you can uninstall AMS^2 from secondary servers.

Installing Symantec AntiVirus servers locally

If the server computer is connected to the network, installing directly from the Symantec AntiVirus CD is the least preferred option because the CD might get damaged or lost, and only one user can install at a time.

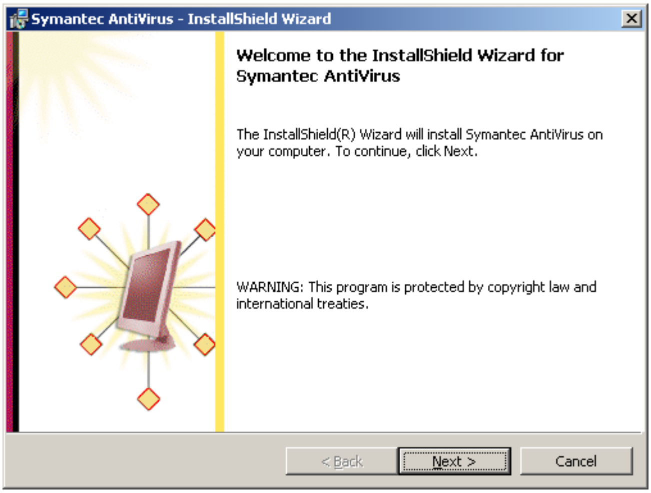
If you make the Symantec AntiVirus CD available on a shared network drive, users must map to that drive on their workstations to ensure the successful installation of all components.

To install a Symantec AntiVirus server locally

1 Do one of the following:

- For installation on a 32-bit computer, in the root of the CD, run Setup.exe.
- For installation on a 64-bit computer, run Setup.exe from the \SAVWIN64 folder.
  Continue to Step 3.

2 In the Symantec AntiVirus panel, click **Install Symantec AntiVirus** > **Install Symantec AntiVirus**.



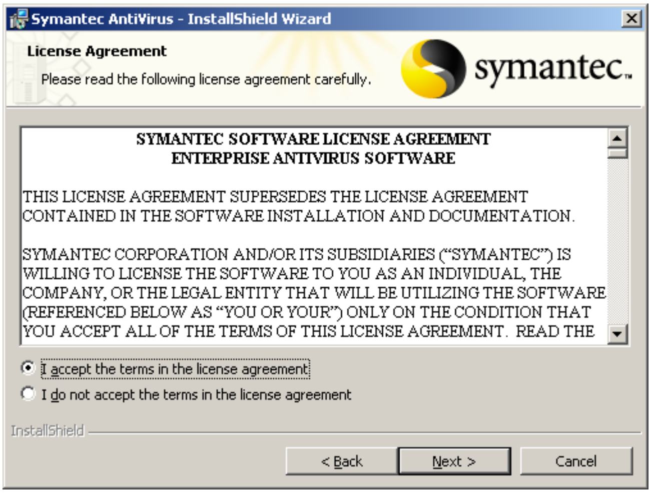
Symantec AntiVirus - InstallShield Wizard

Welcome to the InstallShield Wizard for Symantec AntiVirus

The InstallShield(R) Wizard will install Symantec AntiVirus on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

3 In the welcome panel, click **Next**.



Symantec AntiVirus - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

SYMANTEC SOFTWARE LICENSE AGREEMENT
ENTERPRISE ANTIVIRUS SOFTWARE

THIS LICENSE AGREEMENT SUPERSEDES THE LICENSE AGREEMENT CONTAINED IN THE SOFTWARE INSTALLATION AND DOCUMENTATION.

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

4 In the License Agreement panel, click **I accept the terms in the license agreement**, and then click **Next**.

5 In the Client Server Options panel, click **Server**, and then click **Next**.

6 In the Setup Type panel, select one of the following:

- Complete: To install all of the components that are included with the default installation.
- Custom: To exclude components from the installation or to change the installation location.

7 Click **Next**.

8 In the Select Server Group panel, do one of the following:

- Type the name of an existing Server Group, type the password for that group, and then click **Next**.
- Type the name of a new server group to be created, type the password, and then click **Next**. In the password confirmation dialog box, retype the password.

9 In the Install Options panel, check one of the following:

- Auto-Protect: To enable Auto-Protect
- Run LiveUpdate: To run LiveUpdate at the end of the installation

10 Click **Next**.

11 In the Ready to Install the Program panel, click **Install**.

12 If you chose to run LiveUpdate after installation, do the following:

- Follow the instructions in the LiveUpdate Wizard.
- When LiveUpdate is done, click **Finish**.

13 In the Symantec AntiVirus panel, click **Finish**.

Deploying the server installation across a network connection

To push the Symantec AntiVirus server installation to computers across your network, complete the tasks that are listed in Table 6-2. You should complete each task in the order in which it is listed. The final task is required for NetWare servers only.

Table 6-2 Task list for installing servers across a network

Task	For more information
Start the installation.	See "Starting the server installation" on page 112.
Run the server setup program.	See "Running the server setup program" on page 114.
Select the computers to which you want to install the server program.	See "Selecting computers to which you want to install" on page 116.
Complete the server installation.	See "Completing the server installation" on page 119.
Review any errors.	See "Checking for errors" on page 122.
Start Symantec AntiVirus NLMs.	See "Manually loading the Symantec AntiVirus NLMs" on page 123.

Starting the server installation

You can install the Symantec AntiVirus server from the Symantec AntiVirus CD or the Symantec System Center.

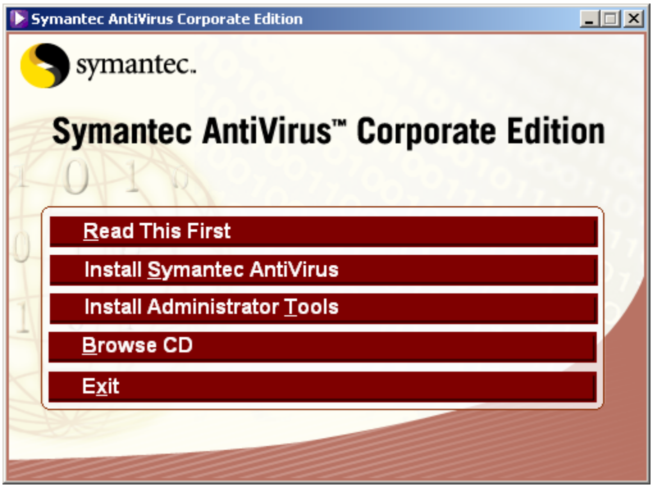
Note: When you are installing to NetWare, log on to all of the NetWare servers before you start the installation. To install to NetWare Directory Services (NDS) or bindery, you need administrator or supervisor rights.

Start the server installation

You can start the server installation from the Symantec AntiVirus CD or from the Symantec System Center.

To start the installation from the CD

1 Insert the Symantec AntiVirus CD into the CD-ROM drive.


Symantec AntiVirus Corporate Edition
symantec.
Symantec AntiVirus™ Corporate Edition
Read This First
Install Symantec AntiVirus
Install Administrator Tools
Browse CD
Exit

2 Click **Install Symantec AntiVirus** > **Deploy AntiVirus Server**.

3 Continue the installation.
See "Running the server setup program" on page 114.

To start the installation from the Symantec System Center

1 In the Symantec System Center, in the left pane, do one of the following:
   - Click **System Hierarchy**.
   - Under System Hierarchy, select any object.

2 On the Tools menu, click **AV Server Rollout**.
AV Server Rollout is available only if you selected the Server Rollout component when you installed the Symantec System Center. This component is selected for installation by default.

3 Continue the installation.
See "Running the server setup program" on page 114.

Running the server setup program

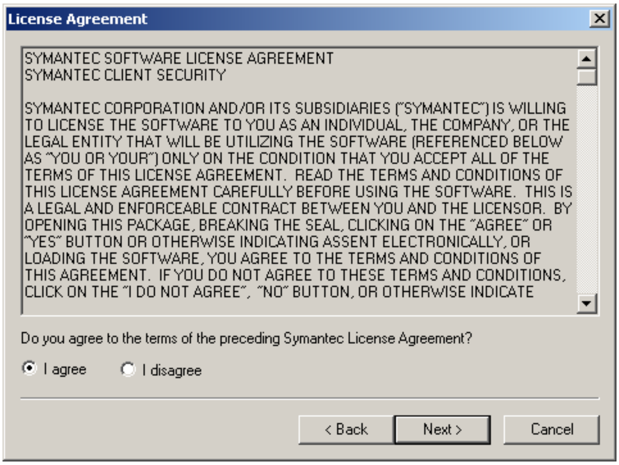
The same setup program runs no matter how you started the installation.

See "Starting the server installation" on page 112.

To run the server setup program

1 In the welcome panel, do one of the following:

- To install the server to computers that have never had Symantec AntiVirus installed, click **Install**, and then click **Next**.
- To install the server to computers that have had Symantec AntiVirus previously installed, click **Update**, and then click **Next**.



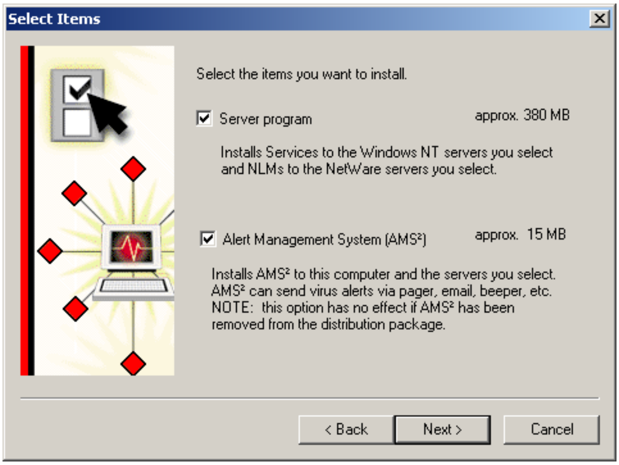
SYMANTEC SOFTWARE LICENSE AGREEMENT
SYMANTEC CLIENT SECURITY

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE

Do you agree to the terms of the preceding Symantec License Agreement?

● I agree ○ I disagree

2 In the License Agreement panel, click **I agree**, and then click **Next**.



Select Items

Select the items you want to install.

☑ Server program approx. 380 MB

Installs Services to the Windows NT servers you select and NLMs to the NetWare servers you select.

☑ Alert Management System (AMS²) approx. 15 MB

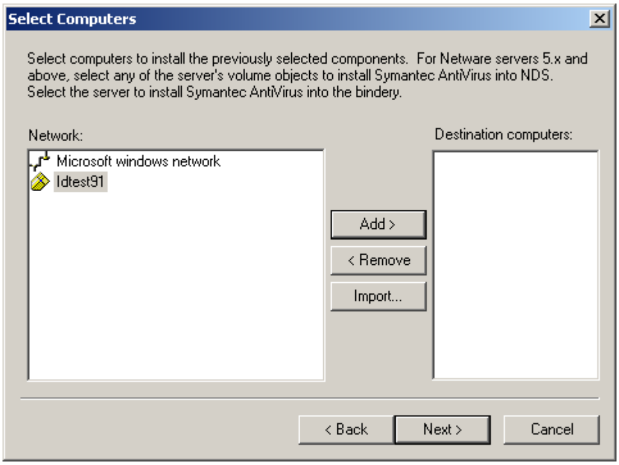
Installs AMS² to this computer and the servers you select. AMS² can send virus alerts via pager, email, beeper, etc. NOTE: this option has no effect if AMS² has been removed from the distribution package.

3 In the Select Items panel, ensure that Server program is checked.

If you plan to use Alert Management System^2 (AMS^2), ensure that it is checked.

See “Why AMS is installed with Symantec AntiVirus server” on page 109.

4 Click **Next**.



Select Computers

Select computers to install the previously selected components. For Netware servers 5.x and above, select any of the server's volume objects to install Symantec AntiVirus into NDS. Select the server to install Symantec AntiVirus into the bindery.

Network:

Microsoft windows network
ldtest91

Destination computers:

5 Continue the installation.

See “Selecting computers to which you want to install” on page 116.

Selecting computers to which you want to install

You can install to one or more computers. In a WINS environment, you can view the computers to which you can install. If you are installing in a non-WINS environment, you must select computers by importing a text file that contains the IP addresses of the computers to which you want to install. You can use the same import method in a WINS environment.

When you install to NDS, the computer that is performing the installation must use the Novell Client for NetWare. If you encounter problems installing to a bindery server with the Microsoft Client for NetWare, install the Novell Client for NetWare and try again.

Note: The Import feature is designed for use with Windows NT-based computers only. It is not intended for use with NetWare.

Select computers to which you want to install

You can select Windows or NetWare computers manually or import a list of computers.

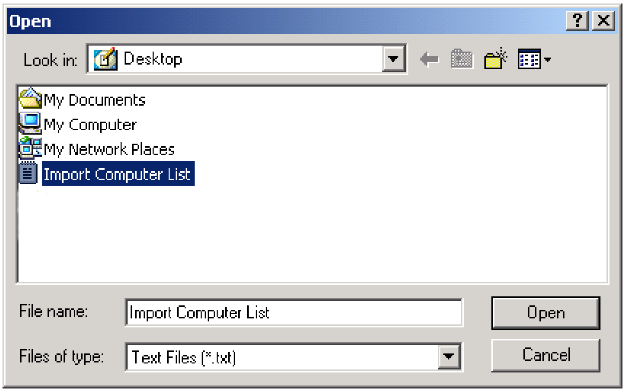
To manually select Windows computers

1. In the Select Computers panel, under Network, expand **Microsoft windows network**.
2. Select a server on which to install, and then click **Add**.
3. Repeat step 2 until all of the servers to which you are installing are added under Destination computers.
4. Select any NetWare computers to which you want to install.
   See "To manually select Novell NetWare computers" on page 118.
5. Continue the installation.
   See "Completing the server installation" on page 119.

To import a list of Windows NT/2000/XP/2003 computers

1. Prepare the list of servers to import.
   See "Creating a text file with IP addresses to import" on page 60.

2 In the Select Computers panel, click **Import**.

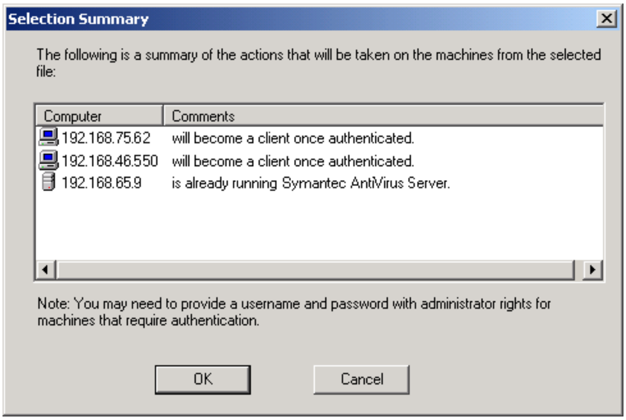


Look in: Desktop

File name: Import Computer List

Files of type: Text Files (*.txt)

3 Locate and double-click the text file that contains the IP addresses to import.



The following is a summary of the actions that will be taken on the machines from the selected file:

Computer	Comments
192.168.75.62	will become a client once authenticated.
192.168.46.550	will become a client once authenticated.
192.168.65.9	is already running Symantec AntiVirus Server.

Note: You may need to provide a username and password with administrator rights for machines that require authentication.

During the authentication process, you may need to provide a user name and password for computers that require authentication.

4 If you are installing to multiple computers, in the Selection Summary dialog box, click **OK**.

If you are installing to a single computer, the Selection Summary dialog box does not appear.

During the authentication process, the setup program checks for error conditions. You are prompted to view this information on an individual computer basis or to write the information to a log file for later viewing.

5 Select one of the following:

- Yes: Write to a log file.
  If you create a log file, it is located under C:\Winnt\Savcesrv.txt.
- No: Display the information on an individual computer basis.

6 Select any NetWare computers to which you want to install.
See "To manually select Novell NetWare computers" on page 118.

7 Continue the installation.
See "Completing the server installation" on page 119.

To manually select Novell NetWare computers

1 In the Select Computers panel, under Available Computers, double-click **NetWare Services**.

2 Do one of the following:

- To install to a bindery server, double-click **NetWare Servers**, and then select a server (indicated by a server icon).
- To install to NDS, double-click **Novell Directory Services**, and then select the SYS volume object in which you want to install Symantec AntiVirus.
  To locate a SYS volume object, double-click the tree object and continue expanding the organizational objects until you reach the organizational unit that contains the SYS volume object.

3 Click **Add**.

4 If you are installing to NDS, you are prompted to type a container, user name, and password.
If you type an incorrect user name or password, the installation will continue normally. However, when you attempt to start Symantec AntiVirus on the NetWare server, you will receive an authentication error and be prompted for the correct user name and password.

5 Repeat steps 1 through 4 until the volumes for all of the servers that you are installing to are added under AntiVirus Servers.

6 Select any Windows computers to which to install.
See "To manually select Windows computers" on page 116.
See "To import a list of Windows NT/2000/XP/2003 computers" on page 116.

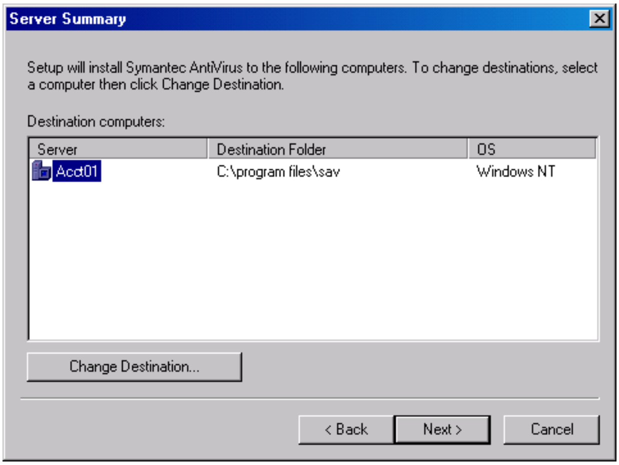
7 Continue the installation.
See "Completing the server installation" on page 119.

Completing the server installation

After you have selected the computers to which you want to install, you can complete the installation. All of the computers are added to the same server group, but you can create new server groups and move servers to them in the Symantec System Center.

To complete the server installation

1 In the Select Computers panel, click **Finish**.



Server Summary

Setup will install Symantec AntiVirus to the following computers. To change destinations, select a computer then click Change Destination.

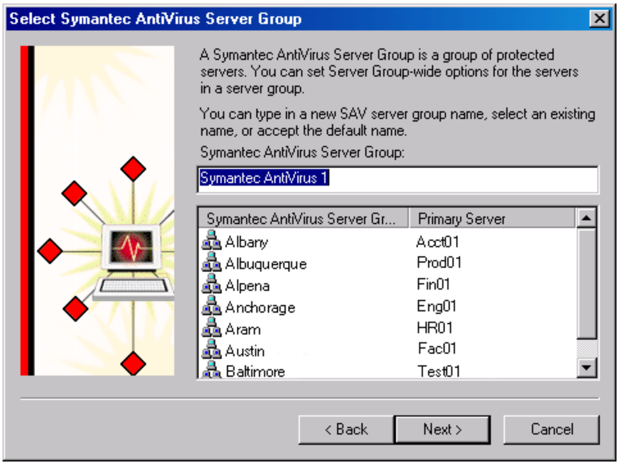
Destination computers:

Server	Destination Folder	OS
Acct01	C:\program files\sav	Windows NT

2 In the Server Summary panel, do one of the following:

- To accept the default Symantec AntiVirus installation path, click **Next**.
- To change the path, select a computer, and then click **Change Destination**. In the Change Destination dialog box, select a destination, click **OK**, and then click **Next**.

If you are installing to a NetWare server, the new folder name is limited to eight characters.



Select Symantec AntiVirus Server Group

A Symantec AntiVirus Server Group is a group of protected servers. You can set Server Group-wide options for the servers in a server group.

You can type in a new SAV server group name, select an existing name, or accept the default name.

Symantec AntiVirus Server Group:

Symantec AntiVirus 1

Symantec AntiVirus Server Gr...	Primary Server
Albany	Acct01
Albuquerque	Prod01
Alpena	Fin01
Anchorage	Eng01
Aram	HR01
Austin	Fac01
Baltimore	Test01

3 In the Select Symantec AntiVirus Server Group panel, do one of the following:

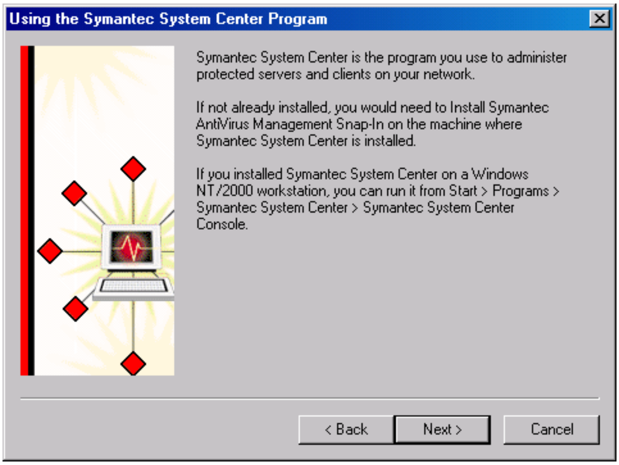
- Under Symantec AntiVirus Server Group, type a name for a new server group, and then click **Next**.
  You will be prompted to confirm the creation of the new server group and to specify a password for the server group.
- In the list, select an existing server group to join, click **Next**, and then type the server group password when you are prompted.

4 Select one of the following:

- Automatic startup: On a NetWare server, you must manually load Vpstart.nlm after you install Symantec AntiVirus server, but Vpstart.nlm will load automatically thereafter. (You must either create or join a server group during the installation process before this takes effect.)
  On a Windows NT-based computer, Symantec AntiVirus services (and AMS^2 services, if you installed AMS^2) start automatically every time that the computer restarts.
- Manual startup: On a NetWare server, you must manually load Vpstart.nlm after you install Symantec AntiVirus server and every time that the server restarts. Selecting this option will have no effect on Windows computers.

See "Manually loading the Symantec AntiVirus NLMs" on page 123.

5 Click **Next**.



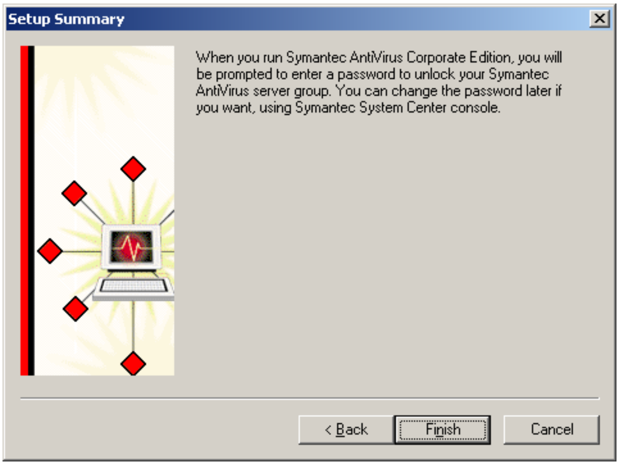
Using the Symantec System Center Program

Symantec System Center is the program you use to administer protected servers and clients on your network.

If not already installed, you would need to Install Symantec AntiVirus Management Snap-In on the machine where Symantec System Center is installed.

If you installed Symantec System Center on a Windows NT/2000 workstation, you can run it from Start > Programs > Symantec System Center > Symantec System Center Console.

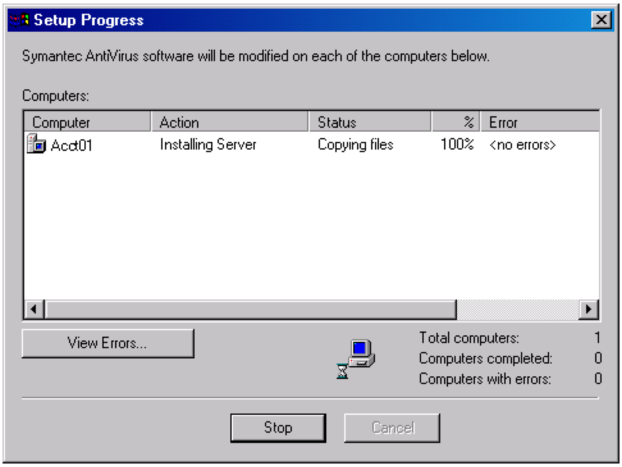
6 In the Using the Symantec System Center Program panel, click **Next**.



Setup Summary

When you run Symantec AntiVirus Corporate Edition, you will be prompted to enter a password to unlock your Symantec AntiVirus server group. You can change the password later if you want, using Symantec System Center console.

7 In the Setup Summary panel, read the message that reminds you that you will need your password to unlock the server group in the Symantec System Center, and then click **Finish**.



Symantec AntiVirus software will be modified on each of the computers below.

Computers:

Computer	Action	Status	%	Error
Acct01	Installing Server	Copying files	100%	<no errors>

Total computers: 1
Computers completed: 0
Computers with errors: 0

8 In the Setup Progress panel, view the status of the server installations.

9 Finish the installation.
See “Checking for errors” on page 122.

Checking for errors

When Symantec AntiVirus server is installed to all of the computers that you specified, you can check to see if any errors were reported.

To check for errors

1 In the Setup Progress panel, select a server, and then click **View Errors**.

2 When you are done, click **Close.**

Note: When installing to a Windows NT computer, you must restart the computer when the installation completes.

If you’ve installed to any NetWare computers, you need to load the appropriate NLMs.

See “Manually loading the Symantec AntiVirus NLMs” on page 123.

Manually loading the Symantec AntiVirus NLMs

After you install the Symantec AntiVirus server software, you must run Vpstart.nlm on each NetWare server to complete the installation. You can do this at the server console if you have rights, or by using RConsole (NetWare 5.x) for IPX protocol networks or RConsoleJ (NetWare 5.x/6) for IP protocol networks.

Manually load the Symantec AntiVirus NLMs

After installation, you must use the /Install switch to load Vpstart.nlm for the first time. If you selected automatic startup during installation, the NLMs will load automatically the next time that the server restarts. If you selected manual startup, you must manually load Vpstart.nlm every time that you restart the server.

Note: At the NetWare console, do not add the path to the command specified. Type the command exactly as it appears. These NetWare commands are case-sensitive.

To manually load the Symantec AntiVirus NLMs for the first time

◆ At the server console, type the following:

```
Load Sys:Sav\Vpstart.nlm /Install
```

Warning: You only need to perform this procedure one time after software installation. If you use the /Install switch again, you will overwrite any current configuration settings.

To manually load the Symantec AntiVirus NLMs after NLM installation

◆ At the server console, type the following:

```
Vpstart.nlm
```

Installing Symantec AntiVirus with NetWare Secure Console enabled

If you are using NetWare Secure Console, you can install Symantec AntiVirus while Secure Console is running. After you perform a standard Symantec AntiVirus installation, you must copy the NLM to the appropriate directory and then run the NLM on each NetWare server to complete the installation. You can do this at the server console if you have rights, or by using RConsole (NetWare 5.x) for IPX protocol networks or RConsoleJ (NetWare 5.x/6) for IP protocol networks.

Install Symantec AntiVirus with NetWare Secure Console enabled

After installation, you must copy Vpstart.nlm from the installation directory to the Sys:\System directory and then use the /Install switch to load Vpstart.nlm for the first time. If you selected automatic startup during installation, the NLMs will load automatically the next time that the server restarts. If you selected manual startup, you must manually load Vpstart.nlm every time that you restart the server.

Note: At the NetWare console, do not add the path to the commands specified. Type each command exactly as it appears. These NetWare commands are case-sensitive.

To manually load the Symantec AntiVirus NLMs for the first time while running NetWare Secure Console

1. From the Sys:\Sav default installation directory (or the directory that was specified during installation), copy **Vpstart.nlm** to the Sys:\System directory.
2. At the server console, type the following:

   ```
   Vpstart /install /SECURE_CONSOLE SYS:\SAV\VPSTART.NLM
   ```

   Warning: You only need to perform this procedure one time after software installation. If you use the /Install switch again, you will overwrite any current configuration settings.

To manually load the Symantec AntiVirus NLMs after NLM installation while running NetWare Secure Console

◆ At the server console, type the following:

```
Vpstart.nlm
```

Installing directly to a Windows computer using the server installation package

The Windows Installer (.msi) antivirus server installation package (Setup.exe) that comes with Symantec AntiVirus can be used to install directly to a supported Windows computer by executing the installation program manually or through other deployment methods, such as distributing and executing the installation using a third-party tool.

See "Installing Symantec AntiVirus using command-line parameters" on page 161.

Direct installation requires users to be logged on to the computer with administrative rights. The only exception to this is if you have enabled elevated privileges for Windows Installer packages through the Microsoft Management Console.

See "How to deploy to a target computer without granting administrator privileges" on page 62.

The installation package and the supporting files must be copied to a location from which they can be run. When the package is opened, the server installation starts.

To place the installation package in a location from which it can be run

1. On the Symantec AntiVirus CD, copy the contents of the \Rollout\AVServer folder to the location that you want.
2. Distribute the Windows Installer files using your preferred deployment method.
3. Run the installation program (Setup.exe).

Manually installing AMS server

You can manually install AMS^2 server to computers to which you've already installed Symantec AntiVirus server.

Manually install AMS server

The installation methods for AMS^2 are different for Windows NT-based computers and NetWare servers.

Note: To avoid losing valuable information when you uninstall Symantec AntiVirus from a primary server running under NetWare, first demote the primary server from which you are uninstalling to secondary status and then promote a new server to primary status. For more information on selecting primary servers, see the *Symantec AntiVirus Administrator's Guide*.

To manually install AMS^2 server to Windows NT/2000/XP/2003 computers

1. Insert the Symantec AntiVirus CD into the CD-ROM drive.
2. Run the Setup.exe program, which is located in the following directory:
   Rollout\AVServer\Ams2\Winnt
3. Follow the on-screen instructions.

To manually install AMS^2 server to NetWare servers

1. Uninstall the Symantec AntiVirus server.
   See "Uninstalling Symantec AntiVirus server" on page 126.
2. Run the server setup program.
   See "Running the server setup program" on page 114.
3. When prompted, ensure that Alert Management System^2 (AMS^2) is checked.

Uninstalling Symantec AntiVirus server

You should uninstall Symantec AntiVirus servers and clients using the automatic uninstallation program that is provided by Symantec. If a manual uninstallation is required, see the support Knowledge Base on the Symantec Web site.

If a Symantec AntiVirus server is managing Symantec AntiVirus clients and you plan to uninstall and then reinstall the Symantec AntiVirus server software, ensure that the computer to which you reinstall has the same computer name and IP address. If this information changes, clients will not be able to locate their parent server.

If you don't plan to replace a Symantec AntiVirus server that is managing Symantec AntiVirus clients, you should reassign any clients that are managed by the server before you uninstall the Symantec AntiVirus server software. For more information, see the *Symantec AntiVirus Administrator's Guide*.

Uninstall Symantec AntiVirus server

You can uninstall Symantec AntiVirus server from computers running supported Microsoft Windows operating systems and NetWare computers.

Note: To avoid losing valuable information when you uninstall Symantec AntiVirus from a primary server running under NetWare, first demote the primary server from which you are uninstalling to secondary status and then promote a new server to primary status. For more information on selecting primary servers, see the *Symantec AntiVirus Administrator's Guide*.

To uninstall Symantec AntiVirus server from a computer running a supported Windows operating system

1. On the Windows taskbar, click **Start** > **Settings** > **Control Panel.**
2. In the Control Panel window, double-click **Add/Remove Programs**.
3. In the Add/Remove Programs dialog box, click **Symantec AntiVirus Server**.
4. Click **Remove**.

To uninstall Symantec AntiVirus server from NetWare computers

1. To switch to the Symantec AntiVirus Corporate Edition screen on the server, press **Ctrl+Esc**, and then click **Symantec AntiVirus Corporate Edition**.
2. To unload the NLMs, press **Alt+F10**.
3. At the server console, at the command prompt, type the following:

```
load Sys:\sav\Vpstart.nlm /remove
```

Chapter 7

Installing Symantec AntiVirus clients

This chapter includes the following topics:

Client installation methods

You can install Symantec AntiVirus client using any of the methods that are listed in Table 7-1. You can use any combination of methods that suits your network environment.

Table 7-1 Client installation methods

Method	Description	Preparation
Push	You can push the Symantec AntiVirus client installation directly from the Symantec AntiVirus CD or from the Symantec System Center. This method lets you install on computers running supported Microsoft Windows operating systems without giving users administrative rights to their computers. See "Deploying the client installation across a network connection" on page 133.	Install the Symantec System Center with the antivirus management snap-in, and use the NT Client Install tool to push the client installation from the Symantec System Center.
Logon script	You can fully automate client installations and updates by using logon scripts. See "Setting up client installations using logon scripts" on page 137.	For legacy client installation requirements, see the *Norton AntiVirus Corporate Edition Implementation Guide* that came with your legacy software.
From a server	You can run a Symantec AntiVirus client installation package from the Symantec AntiVirus server that you want to act as a parent server. See "Installing from the client installation package on the server" on page 141.	■ Install Symantec AntiVirus server. ■ Have users map a drive to the VPHOME\clt-inst\WIN32 share on Symantec AntiVirus server to ensure a successful installation.
Web	Users download a client installation package from an internal Web server, and then run it. This option is available for computers that are running a supported Windows operating system. See "Deploying installation packages using Web-based deployment" on page 142.	■ Ensure that the Web server meets the minimum requirements. ■ Prepare the internal Web server for deployment. ■ Copy the default client installation files to the Web server or create a custom installation package, if desired. ■ For legacy client installation requirements, see the *Norton AntiVirus Corporate Edition Implementation Guide* that came with your legacy software.

Table 7-1 Client installation methods

Method	Description	Preparation
Local	You can run the installation directly from the Symantec AntiVirus CD. This is the primary installation method supported for 64-bit computers. See "Installing Symantec AntiVirus clients locally" on page 150.	Copy the configurations file (Grc.dat) from the parent server to the client computer.
Third-party tools	You can use a variety of third-party installation tools to distribute the Windows Installer-based installation files or a package that you've created with Symantec Packager that includes the preconfigured installation package. Customizing the Windows Installer installation packages using Symantec Packager is not supported. **Note:** Symantec Packager is included with this release of Symantec AntiVirus as an unsupported tool. For more information, see *Using Symantec Packager with Symantec AntiVirus* (pkgrinfo.pdf) in the Symantec Packager folder on the Symantec AntiVirus CD. See "About installing clients using third-party products" on page 154.	■ See the documentation that came with your third-party installation tool for instructions on using the tool. ■ Create a custom .msi installation using the components and options specific to Symantec AntiVirus installation packages. See "Windows Installer (.msi) command-line reference" on page 161.
NetWare server automatic installations	You can configure Symantec AntiVirus to install automatically to your Windows clients from NetWare servers. See "Configuring automatic client installations from NetWare servers without the Symantec System Center" on page 156.	Install Symantec AntiVirus server on the NetWare server.

About Symantec AntiVirus client installation

The Symantec AntiVirus client program does the following:

- Protects the computer on which it runs
- If managed, communicates with its Symantec AntiVirus parent server

Symantec AntiVirus client runs on supported computers that may act as network servers or workstations. If a Windows network server needs antivirus protection only, install the Symantec AntiVirus client.

You can install Symantec AntiVirus using any of the following methods:

- Deploy the client installation package across a network connection to remote computers from the Symantec System Center or the Symantec AntiVirus CD.
  See "Deploying the client installation across a network connection" on page 133.
- Distribute the client installation package to the computer on which it is to be installed, and then execute the package. Common distribution methods include the following:
  - Run a logon script.
  - Run from the client installation folder on the Symantec AntiVirus server.
  - Download from an internal Web site.
  - Run directly from the Symantec AntiVirus CD.

See "Symantec AntiVirus client installation requirements" on page 73.

About the client configurations file

If you want the client to report to a specific parent server, you must do one of the following:

- Copy the appropriate configurations file (Grc.dat) to the client after it has been installed.
  See "Configuring clients using the configurations file" on page 158.
- Install the client using the .msi command-line parameter that specifies the parent server.
  See "Windows Installer (.msi) command-line reference" on page 161.
- Use Symantec Packager to create a custom installation package that contains both a Windows Installer package and the appropriate configurations file. Customizing the Windows Installer installation packages using Symantec Packager is not supported.

  Note: Symantec Packager is included with this release of Symantec AntiVirus as an unsupported tool. See *Using Symantec Packager with Symantec AntiVirus* (pkgrinfo.pdf) in the Symantec Packager folder on the Symantec AntiVirus CD.

  - Client Server options: Click **Client**.

Deploying the client installation across a network connection

You can remotely install the Symantec AntiVirus client to computers running supported Microsoft Windows operating systems that are connected to the network. You can install to multiple clients at the same time without having to visit each workstation individually.

An advantage to remote installation is that users do not need to log on to their computers as administrators prior to the installation if you have administrator rights to the domain to which the client computers belong.

To push the Symantec AntiVirus client installation to computers across your network, complete the following tasks in the order in which they are listed:

- Start the client installation.
  See "Starting the client installation" on page 134.
- Run the client setup program.
  See "Running the client setup program" on page 134.

Starting the client installation

You can install the Symantec AntiVirus client using the NT Client Install tool.

Start the client installation

You can install the Symantec AntiVirus client from the Symantec AntiVirus CD or from the Symantec System Center.

To start the client installation from the CD

1. Insert the Symantec AntiVirus CD into your CD-ROM drive.
2. In the Symantec AntiVirus panel, click **Install Symantec AntiVirus > Deploy AntiVirus Client to NT/2000/XP**.
3. Continue the installation.
   See "Running the client setup program" on page 134.

To start the client installation from the Symantec System Center

1. In the Symantec System Center, in the left pane, do one of the following:
   - Click **System Hierarchy**.
   - Under System Hierarchy, select any object.
2. On the Tools menu, click **NT Client Install**.
   NT Client Install is available only if you selected the NT Client Install tool when you installed the Symantec System Center. This component is selected for installation by default.
3. Continue the installation.
   See "Running the client setup program" on page 134.

Running the client setup program

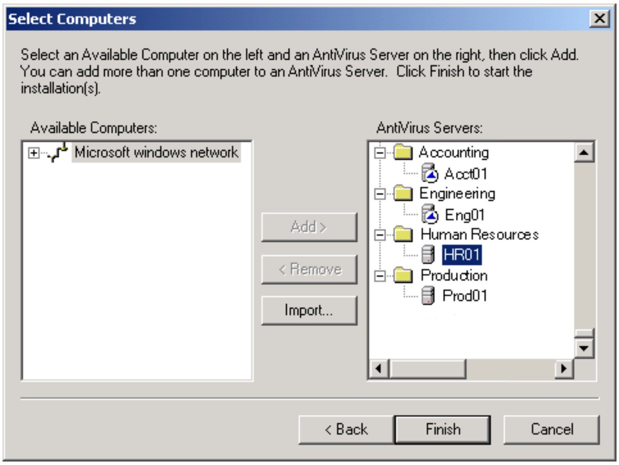
The client setup program runs after you start the installation process.

See "Starting the client installation" on page 134.

To run the client setup program

1. In the welcome panel, click **Next**.
2. In the Select Install Source Location panel, select the location from which you are deploying the client installation files.

3 After you have selected the location, click **Next**.

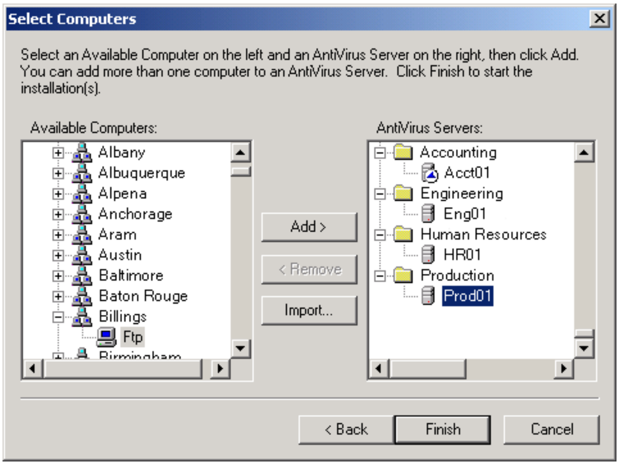

Select Computers

Select an Available Computer on the left and an AntiVirus Server on the right, then click Add. You can add more than one computer to an AntiVirus Server. Click Finish to start the installation(s).

4 In the Select Computers panel, under AntiVirus Servers, select a computer to act as the parent server.

5 Under Available Computers, expand **Microsoft windows network**, and then select a computer.

6 Click **Add**.


Select Computers

Select an Available Computer on the left and an AntiVirus Server on the right, then click Add. You can add more than one computer to an AntiVirus Server. Click Finish to start the installation(s).

7 Repeat steps 5 and 6 until all of the clients that you want to manage are added.

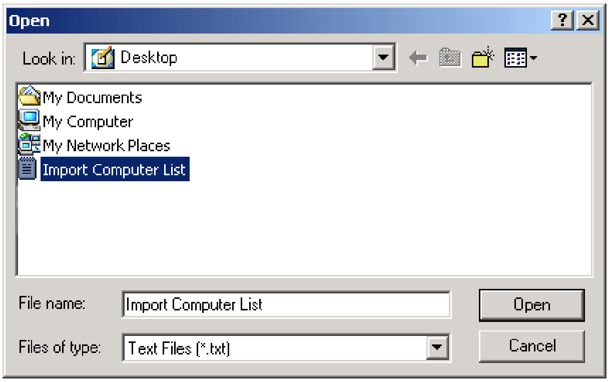
You can reinstall to computers that are already running Symantec AntiVirus. You can also import a text file to add Windows NT-based clients.

8 Do one of the following:

- If you created a text file that contains IP addresses to import computers that are in non-WINS environments, continue to step 9.
- If you did not create a text file that contains IP addresses to import computers in non-WINS environments, continue to step 11.

See "Creating a text file with IP addresses to import" on page 60.

9 To import the list of computers, click **Import**.



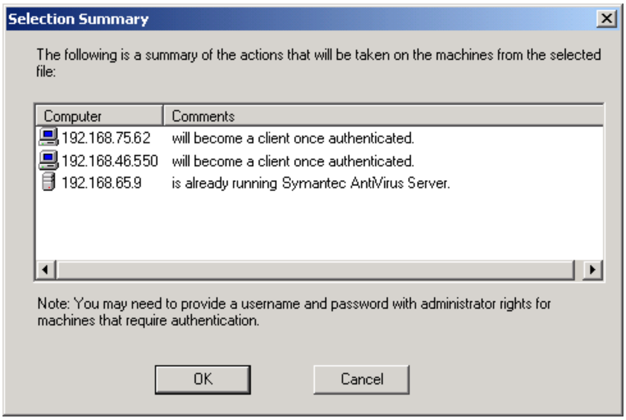
Look in: Desktop

My Documents
My Computer
My Network Places
Import Computer List

File name: Import Computer List

Files of type: Text Files (*.txt)

10 Locate and double-click the text file that contains the computer names.



The following is a summary of the actions that will be taken on the machines from the selected file:

Computer	Comments
192.168.75.62	will become a client once authenticated.
192.168.46.550	will become a client once authenticated.
192.168.65.9	is already running Symantec AntiVirus Server.

Note: You may need to provide a username and password with administrator rights for machines that require authentication.

A summary list of computers to be added under Available Computers appears.

During the authentication process, you may need to provide a user name and password for computers that require authentication.

11 In the Selection Summary dialog box, click **OK**.
During the authentication process, Setup checks for error conditions. You are prompted to view this information interactively on an individual computer basis or to write the information to a log file for later viewing.
If you create a log file, it is located under C:\Winnt\Savcecln.txt.

12 Select one of the following:
   - Yes: Display the information.
   - No: Write to a log file.

13 In the Select Computers panel, click **Finish**.

14 In the Status of Remote Client Installations window, click **Done**.

Setting up client installations using logon scripts

You can automate client installations using the logon scripts that the Symantec AntiVirus server installation program copies to each Symantec AntiVirus server.

When users who are enabled to run the script log on to a protected server, the script calls a program to check the version number of the client that is currently available on the server. If the client version on the server is earlier than the client version on the user's hard disk, or if the client is not installed on the user's hard disk, the client setup program runs for the platforms that you specify.

The server setup program creates a logon group (SymantecAntiVirusUser) on NetWare servers, which simplifies setting up users to run the scripts.

To configure client installation at logon, do the following:

- Use the Symantec System Center to set update options and enable updates.
  See "Setting logon script options in the Symantec System Center" on page 137.
- Use your network administration tools to associate users with the logon script. For Windows logon scripts, you must also copy files from the Symantec AntiVirus server to the netlogon share.
  See "Associating users with the logon script" on page 139.

Setting logon script options in the Symantec System Center

In the Symantec System Center, you configure the installation actions that you want to occur when the user logs on to the client computer.

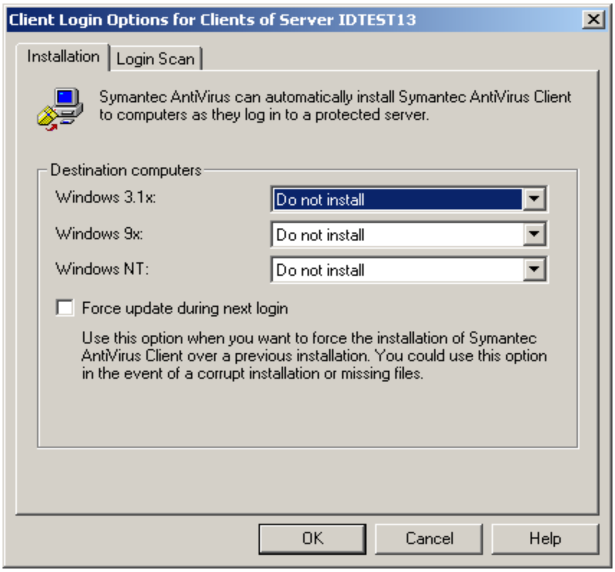
To set logon script options in the Symantec System Center

1. In the Symantec System Center console, right-click a server, and then click **All Tasks** > **Symantec AntiVirus** > **Client Login Scan And Installation**.

   These settings apply to all of the client computers that connect to that server.

2. In the Client Login Options for Clients of Server dialog box, on the Installation tab, set one of the following client logon installation options for each computer type:

   - Automatically install: The user has no option to cancel the installation at logon.
   - Ask the user: The user types Yes or No to receive the installation at logon.
   - Do not install: No changes are made to the client computer at logon.



Symantec AntiVirus can automatically install Symantec AntiVirus Client to computers as they log in to a protected server.

Destination computers

Windows 3.1x: Do not install

Windows 9x: Do not install

Windows NT: Do not install

□ Force update during next login

Use this option when you want to force the installation of Symantec AntiVirus Client over a previous installation. You could use this option in the event of a corrupt installation or missing files.

For Symantec AntiVirus servers, the Windows 9x setting applies only to Windows 98/Me clients. (Windows 95 is not supported.) The Windows NT setting applies to Windows NT-based clients.

For logon installation support for legacy clients, you must use a legacy Norton AntiVirus Corporate Edition 7.6 server. For more information, see the *Norton AntiVirus Corporate Edition Implementation Guide* that came with the original software that you installed.

3 To force an update of Symantec AntiVirus when the client next logs on, check **Force update during next login**.

This option is useful if you are installing over an installation that is corrupt or missing files.

See "How the Force update during next login option works" on page 139.

The Force update during next login option is unchecked after the update on the client is complete.

4 Click **OK**.

5 Continue setting options for logon scripts.

See "Associating users with the logon script" on page 139.

How the Force update during next login option works

Checking Force update during next login increments a counter under [ClientNumber] in Vp_login.ini on the Symantec AntiVirus server. When the client logs on, it compares this value with the value in its registry under the following key:

HKEY_LOCAL_MACHINE\Software\Intel\LanDesk\VirusProtect6\
CurrentVersion\ClientNumber

Each time that you check Force update during next login, the value under [ClientNumber] in Vp_login.ini increases. If the value does not match the [ClientNumber] value on the client, then the client is updated.

Associating users with the logon script

On NetWare servers, the server setup program creates a user group called SymantecAntiVirusUser. When you add a user to the group, the logon script runs according to the options that you set in the Symantec System Center the next time that the user logs on to the server.

For Windows computers running Symantec AntiVirus server, use the Computer Management tool to assign the Vplogon.bat logon script to a user. When the user logs on, the computer runs the script from the netlogon share on Symantec AntiVirus server, which launches the client installation according to the options that you set in the Symantec System Center.

Associate users with a logon script

The procedure for associating users with a logon script differs for NetWare and Windows.

Note: The procedure for associating users with a logon script is different for NetWare versions prior to 5.x. For more information, see the *Norton AntiVirus Corporate Edition Implementation Guide* in the Docs folder on the CD that came with your legacy software.

To associate NetWare users with a logon script

1. Open the NetWare Administrator utility (Nwadmin32 or ConsoleOne).
2. Double-click the **SymantecAntiVirusUser** group.
3. In the Group dialog box, click **Members**.
4. To add a user to the group, click **Add**.
5. Select the user that you want to add, and then click **OK**.
6. To close the Group dialog box, click **OK**.
   The user is added to the SymantecAntiVirusUser group. The configured logon installation occurs the next time that the user logs on to the protected server from a Novell NetWare client.
7. Close the NetWare Administrator utility.

To associate Windows users with a logon script

1. Copy the following files from the Program Files\Symantec AntiVirus\Logon directory on the protected server to the netlogon share (by default, C:\Winnt\System32\Repl\Import\Scripts for Windows NT and C:\Winnt\Sysvol\Sysvol\Domainname\Scripts for Windows 2000/XP/2003):
   - Vplogon.bat
   - Nbpshpop.exe

   If this share has been changed, copy the files to the directory that you set up as the netlogon share.
2. If you are installing to a Windows domain that has PDC and BDC, copy Vplogon.bat and Nbpshpop.exe to all PDC and BDC locations, or set up replication.
   This prevents a File Not Found error when Windows authenticates to other servers.
3. On the Windows taskbar, click **Start** > **Programs** > **Administrative Tools** > **Computer Management**.

4 In the Computer Management window, expand **System Tools** > **Local Users and Groups** > **Users**, and then double-click the user name that you want to receive a client logon installation.

5 In the User Properties dialog box, click **Profile**.

6 In the logon script box of the User profile, type the following:
Vplogon.bat

7 Click **OK**.

Installing from the client installation package on the server

When you install a Symantec AntiVirus server, the server setup program creates a client installation shared folder on that Symantec AntiVirus server.

On servers running supported Microsoft Windows operating systems, the default shared directory for Symantec AntiVirus server is \\Server\Vphome\Clt-inst. Everyone has read permissions.

On NetWare servers, the default shared directory is \\Server\Sys\Sav\Clt-inst. The setup program also creates a group called SymantecAntiVirusUser. If you add users to this group, they will have the rights that they need (Read and File Scan) to run the client installation program from the client disk image on the server.

When a networked user runs the client installation from the server that will manage it, the client installs in managed mode. When its associated server is selected in the Symantec System Center tree in the left pane, the client displays in the right pane. In the Symantec System Center, you can configure and manage the client.

If you want to make the Symantec AntiVirus client installation package available on a custom shared network drive, users must map to that drive on their workstations to ensure the successful installation of all components. They must also have Read and File Scan rights to that shared folder.

To install from the client installation package on the server

1. Verify that users have rights to the client installation package on the server.
2. Distribute the path to users and, if necessary, include drive mapping instructions to the client installation package.

   For NetWare servers, the default path is \\Server\Sys\Sav\Clt-inst.

   For Windows NT servers, the default share path is \\Server\Vphome\Clt-inst.

   The following installation folder and setup program is available in the Clt-inst folder on each server:

   Clt-inst\Win32\Setup.exe

Deploying installation packages using Web-based deployment

The Symantec AntiVirus client installation program is a Windows Installer-based program that can be deployed using a wide variety of deployment tools, including Web-based deployment tools, that support Windows Installer packages.

Deploying packages through Web-based deployment requires the following steps:

- Review the Web-based deployment requirements.
- Install the Web server, if necessary.
- Set up the installation Web site.
- Customize the deployment files: Files.ini and Start.htm.
- Test the installation.
- Notify users of the download location.

Packages that are created with Symantec Packager are self-extracting executable (.exe) files. The Web-based deployment tool supports the deployment of Symantec Packager packages and Windows Installer (.msi) files. Customizing the Windows Installer installation packages using Symantec Packager is not supported.

Note: Symantec Packager is included with this release of Symantec AntiVirus as an unsupported tool. See *Using Symantec Packager with Symantec AntiVirus* (pkgrinfo.pdf) in the Symantec Packager folder on the Symantec AntiVirus CD.

Web-based deployment requirements

Before you begin to implement a Web-based deployment, you should review the requirements in Table 7-2 for the Web server and the target computer.

Table 7-2 Web server and target computer requirements

Deployment on	Requirements
Web server	■ HTTP Web Server. ■ Microsoft Internet Information Server (IIS) version 4.0/5.0, and Apache HTTP Server version 1.3 or later (UNIX and Linux platforms are also supported).
Target computer	■ Internet Explorer 5.01 Service Pack 2 or later. ■ Browser security must allow ActiveX controls to be downloaded to the target computer. When the installation is complete, the security level can be restored to its original setting. ■ Computer must meet system requirements for the package to be installed. ■ User must be logged on to the computer with the rights that are required for the package to be installed.

About the Web server installation

For additional information on the Web server installation, see the documentation that was supplied with the following products:

- Internet Information Server (IIS) 5.0: Installs by default during a Windows 2000 Professional Server/Advanced Server installation. If the IIS installation option was unchecked when Windows 2000 was installed, use the Windows 2000 installation CD to add the IIS service.
- Internet Information Server (IIS) 4.0: Installs to Windows NT 4.0 from the Microsoft Option Pack for Windows NT 4.0.
- Apache Web Server: Installs to version 1.3 or later, for Windows NT 4.0/2000. (UNIX and Linux platforms are also supported.) The Apache Web Server can be downloaded from the Apache Software Foundation Web site at:
  http://www.apache.org/httpd.html

Setting up the Web server

To set up the Web server, complete the following tasks in the order in which they are listed:

- Copy the installation files to the Web server.
- Configure the Web server.

Alternately, if Symantec AntiVirus server is installed on the Web server, you can copy the files in the Web Install folder to the client installation folder on that server, and then configure the Web server to use the client installation folder as the virtual directory.

Copying the installation files to the Web server

The same procedure is used for Internet Information Server and Apache Web Server.

To copy the installation files to the Web server

1. On the Web server, create a directory called Deploy.
2. Copy the Webinst folder from the Tools folder on the Symantec AntiVirus CD to the Deploy directory.
3. Copy the Grc.dat and installation files to the Deploy\Webinst\Webinst folder on the Web server from one the following locations:
   - The \\Server\Vphome\Clt-inst\Win32 shared folder on the Windows NT-based computer that is running the server that you want to act as the parent server
   - The \\Server\Sys\Sav\Clt-inst\Win32 shared folder on the NetWare Server that is running the server that you want to act as the parent server
4. Ensure that the default document for the virtual directory is Default.htm.

When you are finished, the folder structure on the Web server will look as follows (note that all files are case-sensitive):

- Deploy\Webinst
  - brnotsup.htm
  - default.htm
  - intro.htm
  - logo.jpg
  - oscheck.htm
  - plnotsup.htm

  - readme.htm
  - start.htm
  - webinst.cab
- Deploy\Webinst\Webinst
  - files.ini
  - The installation package (for example, Package.msi)

Configuring the Web server

You must configure the Web server to create a virtual directory.

Configure the Web server

You can configure Internet Information Server or Apache Web Server.

To configure Internet Information Server

1. To launch Internet Services Manager, do one of the following:
   - IIS version 4.0: On the Windows taskbar, click **Start** > **Programs** > **Windows NT 4.0 Option Pack** > **Microsoft Internet Information Server** > **Internet Services Manager**.
   - IIS version 5.0: On the Windows taskbar, click **Start** > **Programs** > **Administrative Tools** > **Internet Services Manager**.
2. Double-click the Web server icon to open it.
3. Right-click **Default Web Site**, and then click **New** > **Virtual Directory**.
4. To begin the Virtual Directory Creation Wizard, click **Next**.
5. In the Alias text box, type a name for the virtual directory (for example, ClientInstall), and then click **Next**.
6. Type the location of the installation folder (for example, C:\Client\Webinst), and then click **Next**.
   The default location is C:\Program Files\SAV\CLT-INST\WEBINST.
7. For access permissions, check **Read only**, and then click **Next**.
8. Right-click the new virtual directory, and then click **Properties**.
9. In the Properties window, on the Virtual Directory tab, change the Execute Permissions to None, and then click **OK**.
10. To complete the virtual directory creation, do one of the following:
    - IIS 4.0: Click **Finish**.
    - IIS 5.0: Click **Next**, and then click **Finish**.

To configure Apache Web Server

1 In a text editor, open **Srm.conf**.
The Srm.conf file is installed by default under C:\Program Files\Apache Group\Apache\conf.

2 Type the following five lines at the end of the Srm.conf file:

```
DirectoryIndex default.htm
<VirtualHost 111.111.111.111>
#ServerName machinename
DocumentRoot "C:\Client\Webinst"
</VirtualHost>
```

For the VirtualHost	Replace 111.111.111.111 with the IP address of the computer on which Apache HTTP Server is installed.
For ServerName	Replace machinename with the name of the server.
For the DocumentRoot	Specify the folder in which you copied the Web installation files (for example, "C:\Client\Webinst"). Double quotation marks are required to specify the DocumentRoot. If the quotation marks are omitted, Apache services might not start.

Customizing the deployment files

Two files must be modified for the deployment. Start.htm resides in the root of the Webinst directory. Files.ini resides in the Webinst subdirectory.

Customize the deployment files

You modify Files.ini to contain the names of the packages that you want to deploy. You can provide the installation options in Table 7-3 by including the InstallOptions keyword in the [General] section.

See “Windows Installer commands” on page 163.

Table 7-3 InstallOptions switches

Switch	Description
/qn	Install silently.
/qb	Install passively.
/l:<log file>	Enable logging, where <log file> is the name of the log file you want to generate. The log file specified must have a .log file extension.

Table 7-3 InstallOptions switches

Switch	Description
/v	Set the level of logging verboseness. The valid values are 0, 1, and 2.

The parameters in the Start.htm file contain information about the Web server and the locations of the files that need to be installed. The configuration parameters in Table 7-4 are located near the bottom of the Start.htm file, inside the <object> tags.

Table 7-4 Start.htm parameters and values

Parameter	Value
ServerName	The name of the server that contains the installation source files. You can use Hostname, IP address, or NetBIOS name. The source files must reside on an HTTP Web server. For example, if your file uses the following object tag, replace ENTER_SERVER_NAME with the computer name or IP address where the installation source files are located: <param name=”ServerName” value=”ENTER_SERVER_NAME”>
VirtualHomeDirectory	The virtual directory of the HTTP server that contains the installation source files. For example, if your file uses the following object tag, replace ENTER_VIRTUAL_HOMEDIRECTORY_NAME with the name of the virtual directory you created (such as Deploy\webinst): <param name=”VirtualHomeDirectory” value=”ENTER_VIRTUAL_HOMEDIRECTORY_NAME”>
ConfigFile	The file name of the Files.ini file. The default value for this parameter does not need to be changed unless you’ve renamed Files.ini.
ProductFolderName	The subdirectory that contains the source files to be downloaded locally. This subdirectory contains the package and Files.ini (for example, Webinst).
MinDiskSpaceInMB	The minimum hard disk space requirement. The default value is appropriate.
ProductAbbreviation	The abbreviation for the product. The default value is appropriate.

To customize Files.ini

1 In a text editor, open **Files.ini**, which is located in the \SAV\Clt-inst\webinst folder by default.

2 In the [Files] section, edit the line File1= so that it references the package that you want to deploy.

For example, in File1=Package.exe, replace Package.exe with the name of the package or .msi file that you want to deploy (usually Setup.exe). Long file names are supported.

3 For each additional file, add a new File*n*= *filename* line, where n is a unique number and filename is the name of the file.

For example, File2=Grc.dat.

4 In the [Files] section, edit the line FileCount= so that it reflects the number of files that you are specifying.

For example, if you included File1, File2, and File3 lines in the [Files] section, FileCount=3.

5 In the [General] section, edit the line LaunchApplication= so that it references the program that you want to start after the download completes. For a package, this is the name of the package.

For example, LaunchApplication= Package.exe.

6 If you want to use additional installation options, add an InstallOptions line after the LaunchApplication line and specify the installation options that you want to include.

For example, InstallOptions=/qn /l:"C:\temp\example.log" /v:2

7 Save **Files.ini**.

Some IIS configurations require that you rename the .ini file using a .txt extension. For more information, see the Symantec Knowledge Base.

To customize Start.htm

1 In a text editor, open **Start.htm**.

2 Search for the <object> tags and type the correct values.

See Table 7-4, "Start.htm parameters and values," on page 147.

To enable the Web installation, the ServerName and VirtualHomeDirectory parameters must be customized to match your Web server configuration.

3 Save **Start.htm**.

Testing the installation

You can test the installation by going to a Web site.

To test the installation

1. Go to a Web site (for example, <your web site>/Webinst), and then click **Install**.
2. If the installation fails, the following types of error messages could be displayed:
   - If there is a problem with the parameters in Start.htm, an error message shows the path of the files that the Web-based installation is trying to access. Verify that the path is correct.
   - If there is a problem in Files.ini (for example, a File not found error), compare the File1= value with the actual name of the package file.
   - Confirm that no other entries were changed during modification.

How to notify users of the download location

You can email instructions to your users to download the package that you want to deploy.

To download the client installation program, users must have Internet Explorer 5.01 Service Pack 2 or later on their computers. The Internet Explorer security level for the local intranet must be set to Medium so that Symantec ActiveX controls can be downloaded to the client. When the installation is complete, the security level can be restored to its original setting.

Make sure that users understand the system requirements and have the administrator rights that are required for the products that they are installing. For example, to install Symantec AntiVirus client, users who are installing to Windows NT-based workstations must have administrator rights on their own computers and must be logged on with administrator rights.

If your package restarts the client computer at the end of the installation, notify your users that they should save their work and close their applications before they begin the installation. For example, the silent client installation on Windows 98 computers restarts the computer at the end of the setup program.

You can include a URL in your email message that points to the client installation as follows:

- For Internet Information Server:
  http://Server_name/Virtual_home_directory/Webinst/
  where Server_name is the name of the Web-based server, Virtual_home_directory is the name of the alias that you created, and Webinst is the folder that you created on the Web server (for example, http://Server_name/Avclientinstall/Webinst/).
- For Apache Web Server:
  http://Server_name/Webinst/
  where Server_name is the name of the computer on which Apache Web Server is installed. The IP address of the server computer can be used in place of the Server_name.

Installing Symantec AntiVirus clients locally

If the client computer is connected to the network, installing directly from the Symantec AntiVirus CD is the least preferred option because the CD might get damaged or lost, and only one user can install at a time. Also, installing Symantec AntiVirus client in managed mode is more difficult because the user must specify a Symantec AntiVirus server to connect to when installing from the CD.

If users do not specify a Symantec AntiVirus server to connect to when they install from the Symantec AntiVirus CD, the Symantec AntiVirus client is installed in unmanaged mode. This means that users are responsible for getting their own virus definitions files and program updates using the Internet.

To change the client's status to managed, use one of the following methods:

- Reinstall the client from the server or use one of the other installation methods.
- Copy the configurations file (Grc.dat) from the intended parent server to the client. (This method is faster and requires fewer resources.)
  See "Configuring clients using the configurations file" on page 158.

If you make the Symantec AntiVirus CD available on a shared network drive, users must map to that drive on their workstations to ensure the successful installation of all components.

Install Symantec AntiVirus clients locally

When you install Symantec AntiVirus client, you start the installation, set up the client as either a managed or unmanaged client, and finish the installation.

To start the installation

1 If users will run the client in managed mode, inform them of the Symantec AntiVirus server to which they will connect.

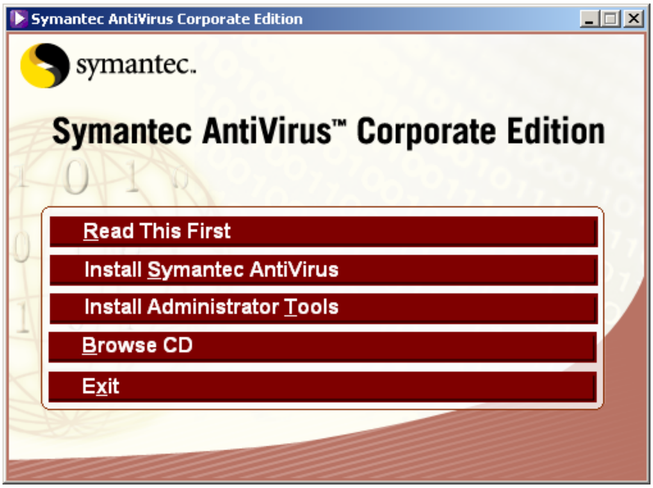
The installation program prompts them for this information.

2 Give users access to the Symantec AntiVirus CD.

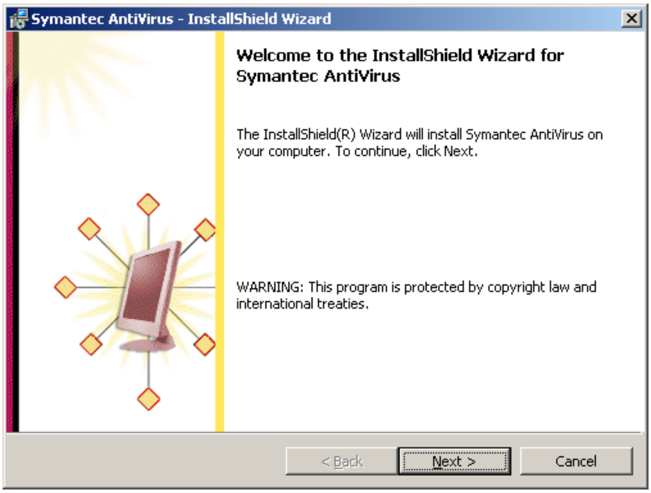
3 Do one of the following:

- For installation on a 32-bit computer, in the root of the CD, have users run Setup.exe.
- For installation on a 64-bit computer, run Setup.exe from the D:\SAVWIN64 folder. Follow the on-screen instructions.

Warning: If the 32-bit version of Setup.exe is run on a 64-bit computer, the installation may fail without notification. For 64-bit installations, run Setup.exe from the \SAVWIN64 folder in the root of the CD.


Symantec AntiVirus Corporate Edition
symantec.
Symantec AntiVirus™ Corporate Edition
Read This First
Install Symantec AntiVirus
Install Administrator Tools
Browse CD
Exit

4 In the Symantec AntiVirus panel, click **Install Symantec AntiVirus > Install AntiVirus Client**.



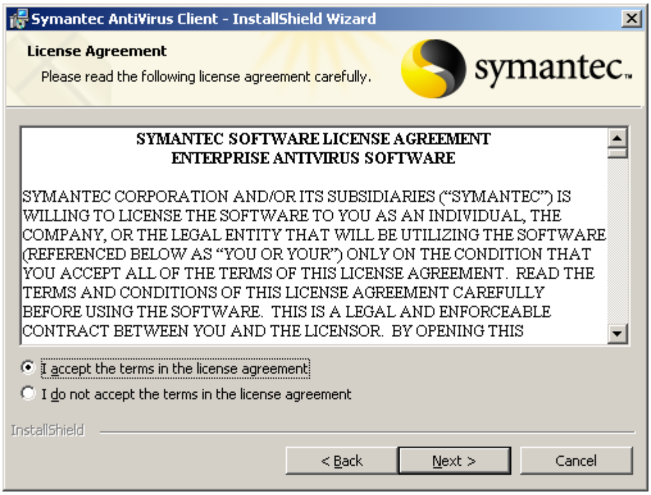
Symantec AntiVirus - InstallShield Wizard

Welcome to the InstallShield Wizard for Symantec AntiVirus

The InstallShield(R) Wizard will install Symantec AntiVirus on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

5 In the welcome panel, click **Next**.



Symantec AntiVirus Client - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

SYMANTEC SOFTWARE LICENSE AGREEMENT
ENTERPRISE ANTIVIRUS SOFTWARE

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

6 In the License Agreement panel, click **I accept the terms in the license agreement**, and then click **Next**.

7 In the Client Server Options panel, click **Client**, and then click **Next**.

8 In the Setup Type panel, select one of the following:

- Complete: To install all of the components that are included with the default installation.
- Custom: To customize the installation.

  For example, in the Custom panel, you can deselect any email protection components that you do not want to install.

9 Click **Next**.

10 In the Network Setup Type panel, do one of the following:

- To have the client be managed by a parent server, click **Managed**, and then click **Next**.

  Continue with "To set up and finish a managed installation" on page 153.
- To have the client run without a parent server, click **Unmanaged**, and then click **Next**.

  Continue with "To finish an unmanaged installation" on page 153.
- If you are migrating from a previous version of Symantec AntiVirus as a managed client, the Network Setup Type panel does not appear.

  Continue with "To finish an unmanaged installation" on page 153.

To set up and finish a managed installation

1 In the Select Server panel, do one of the following:

- In the Server Name text box, type the name, and then click **Next**.
- Click **Browse**, select a server, click **OK** to confirm, and then click **Next**.

  If you don't see the server that you want, click **Find Computer** and search for the computer by name or IP address.

2 In the Ready to Install the Program panel, click **Install**.

To finish an unmanaged installation

1 In the Install Options panel, do the following:

- If you want to enable Auto-Protect, ensure that Auto-Protect is checked.
- If you want to run LiveUpdate at the end of the installation, ensure that LiveUpdate is checked.

2 Click **Next**.

3 In the Ready to Install the Program panel, click **Install**.

4. If you chose to run LiveUpdate after installation, do the following:
   - Follow the instructions in the LiveUpdate Wizard.
   - When LiveUpdate is done, click **Finish**.
5. In the Symantec AntiVirus panel, click **Finish**.

About installing clients using third-party products

You can install Symantec AntiVirus client using a variety of third-party products, including Microsoft Active Directory, Tivoli, Microsoft Systems Management Server (SMS), and Novell ManageWise ZENworks.

About installing clients with Active Directory and Tivoli

You can install Symantec AntiVirus client using the standard options that are provided by Active Directory and Tivoli for all Windows Installer-based installation packages. In addition, Symantec AntiVirus provides a set of properties and features that let you customize the deployment options at the command line.

See “About customizing the client and server installation files using Windows Installer options” on page 58.

For Active Directory and Tivoli deployment instructions, see the documentation on deploying Windows Installer (.msi) installation packages that is provided with the environment that you are using.

About installing clients with Microsoft SMS package definition files

Microsoft SMS administrators can use a package definition file (.pdf) to distribute Symantec AntiVirus to clients. For your convenience, a package definition file (Savce.pdf) is on the Symantec AntiVirus CD in the Tools\Bkoffice folder.

To distribute Symantec AntiVirus with SMS, you typically complete the following tasks:

- Create source directories to store each Symantec AntiVirus component that you plan to distribute.
- Create a query to identify clients that have sufficient free disk space to install the software.
- Create a workstation package to distribute the software.
- Generate an SMS job to distribute and install the workstation package on clients.

In a workstation package, you define the files that comprise the software application to be distributed, and the package configuration and identification information.

The Savce.pdf file has its package configuration and identification information already defined. You can import the file into your workstation package. The installation folder must be copied locally before you run the installation using SMS.

For more information on using SMS, see the Microsoft Systems Management Server documentation.

About installing clients with the Novell ManageWise ZENworks Application Launcher

You can use the Novell ManageWise ZENworks Application Launcher to distribute Symantec AntiVirus client.

After ZENworks is installed on the NetWare server and rolled out to NetWare clients through a logon script, complete the following tasks:

- From Network Administrator, locate an Organization Unit and create an Application Object that points to the location of the Symantec AntiVirus installation files on the server (for example, Sys:\Sav\Clt-inst\Win32\Setup.exe for Windows 98/Me/NT/2000/XP).
- Configure the Application Object. When you set options, you should do the following:
    - Associate the Application Object to an Organization Unit, group of users, or individual users.
    - When you set system requirements, select the operating system that matches the location of the Symantec AntiVirus installation files on the server.
- Set the Application Object installation style. For example, select Show Distribution Progress or Prompt User For Reboot If Needed.

After the preparation is completed, ZENworks pushes the Application Object to the client and launches the setup program when the client logs on. Nothing is required on the client side.

Configuring automatic client installations from NetWare servers without the Symantec System Center

If you have a Novell NetWare server but no Windows NT workstations on which to run the Symantec System Center, you can configure Symantec AntiVirus to install automatically on your Windows clients.

To do this, complete the following tasks:

- Install Symantec AntiVirus on your NetWare server.
  See "Installing to NetWare servers" on page 62.
- Configure automatic installations of Symantec AntiVirus clients on computers running supported Microsoft Windows operating systems.

To configure automatic client installations from NetWare servers

1. Add users to the SymantecAntiVirusUser group using Nwadmin32 or ConsoleOne.
2. On the server console, load Vpregedt.nlm.
3. Click **(O)pen**.
4. Click **VirusProtect6**.
5. Press **Enter**.
6. Click **(O)pen** again, click **LoginOptions**, and then press **Enter**.
7. In the left pane of the window, click **(E)dit** to edit values.
8. Click **DoInstallOnWin95**, and then select one of the following:
   - OPTIONAL: Prompts the user whether to start the installation.
   - FORCE: Silently starts the installation.
   - NONE: Do not install.

   These entries are case-sensitive.
9. If you previously installed clients and need to force a new update, increment the WinNTClientVersion to a higher number.
10. Unload the Symantec AntiVirus NLM from the NetWare server.
11. Type the following command to reload the NLM:
    ```
    Load Sys:\Sav\Vpstart
    ```
12. Test the client installation by logging on as a member of the SymantecAntiVirusUser group from a Novell NetWare client.

Installing the AMS client stand-alone program on an unmanaged client

When you install the Symantec AntiVirus client program, the AMS^2 client software is not installed as part of the client installation. If you want to use the alerting features that AMS^2 provides for unmanaged clients, you can install the AMS^2 client program that is included on the Symantec AntiVirus CD.

To install the AMS^2 client stand-alone program on an unmanaged client

1. In the root of the CD, in the \Rollout\AVServer\AMS2\WINNT folder, run Setup.exe.
2. Follow the on-screen installation instructions.

Post-installation client tasks

After the installation is complete, you may want to perform the following tasks:

- Protect the Symantec AntiVirus registry key on Windows NT 4.0 computers.
  See "How to protect the Symantec AntiVirus registry key on Windows NT 4.0 computers" on page 157.
- Configure clients using the configurations file.
  See "Configuring clients using the configurations file" on page 158.

How to protect the Symantec AntiVirus registry key on Windows NT 4.0 computers

With default permissions set on a Windows NT 4.0 computer, all users can modify the data that is stored in the registry for any application, including Symantec AntiVirus.

To resolve this security problem, remove the permissions that give users open access to the registry. The Reset ACL tool (ResetACL.exe) removes the permissions that allow full access by all users to the following Symantec AntiVirus registry key and subkeys:

HKLM\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion

To use the Reset ACL tool, complete the following tasks:

- Roll out ResetACL.exe, which is located on the Symantec AntiVirus CD in the Tools folder, to Windows NT 4.0 computers that are not secure.
- Run ResetACL.exe on each Windows NT 4.0 computer.

After you run ResetACL.exe, only users with administrator rights can change the registry keys.

Trade-off considerations for the Reset ACL tool

While the Reset ACL tool boosts security for Symantec AntiVirus on Windows NT 4.0 computers, there are several trade-off considerations.

In addition to losing access to the registry, users without administrator rights cannot perform the following operations:

- Start or stop the Symantec AntiVirus Corporate Edition service.
- Run LiveUpdate.
- Schedule LiveUpdate.
- Configure antivirus protection. For example, they cannot set Auto-Protect or email scanning options.
  The options that are associated with these operations are unavailable in the client interface.

Users can modify scan options, but the changes are not saved in the registry nor are they processed. Users can also save manual scan options as the default set, but the options are not written to the registry.

Configuring clients using the configurations file

You may want to use the configurations file (Grc.dat) to configure clients when you do any of the following:

- Install an unmanaged Symantec AntiVirus client.
- Change the parent server of a managed client without having to uninstall and reinstall the client.

To assign the client to a parent server, complete the following tasks in the order in which they are listed:

- Obtain the configurations file.
  See “Obtaining the configurations file” on page 159.
- Copy the configurations file to the client.
  See “Copying the configurations file to the client” on page 159.

Obtaining the configurations file

The configurations file (Grc.dat) contains the name of the server that you want to act as the parent server. If you copy the file from the server that you want to act as the parent server, you will distribute all of the client settings for that server.

Obtain the configurations file

You can copy the configurations file from a server or create a configurations file with the name of the parent server.

To copy the configurations file from a server

1. Open Network Neighborhood or My Network Places.
2. Locate and double-click the computer that you want to act as the parent server.
   Symantec AntiVirus server must be installed on the computer that you select.
3. Open the **VPHOME\Clt-inst\Win32** folder.
4. Copy **Grc.dat** to the desired location.

To create a configurations file with the name of a parent server

1. In a text editor, open a **Grc.dat** file.
   You can find a minimal version of the configurations file on the Symantec AntiVirus CD in the Sample\Tools folder.
2. Search for the following line:
   ```
   PARENT=
   ```
3. Type the letter **S** and the name of your server as follows:
   ```
   PARENT=S<Servername>
   ```
   where <Servername> is the name of your server. (Don’t include the brackets.)
4. Save and close the text file.

Copying the configurations file to the client

You copy the configurations file (Grc.dat) that contains the name of the parent server that will manage the client. You can either copy the file manually or you can use the Microsoft Installer options that are available to create and roll out a package that contains the configurations file.

See “Windows Installer (.msi) command-line reference” on page 161.

To copy the configurations file to the antivirus client

1. Copy the **Grc.dat** file from the desired location.
2. Paste the **Grc.dat** file to one of the following folders on the client:
   - Windows 98/Me: C:\Program Files\Symantec AntiVirus
   - Windows NT 4.0: C:\Winnt\Profiles\All Users\
     Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5
   - Windows 2000/XP/2003: C:\Documents and Settings\All Users\
     Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5
3. Restart the client.
   The configurations file disappears after it is used to update the client.

Uninstalling Symantec AntiVirus clients

You should uninstall Symantec AntiVirus clients using the uninstallation program that is provided by Symantec. You must uninstall Symantec AntiVirus client from the local computer. If a manual uninstallation is required, see the support Knowledge Base on the Symantec Web site.

You can uninstall Symantec AntiVirus client from Windows computers.

Note: During the uninstallation, Windows may indicate that it is installing software. This is a general Microsoft message that can be ignored.

To uninstall the client

1. On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Add/Remove Programs**.
3. In the Add/Remove Programs dialog box, click Symantec AntiVirus **Client**.
4. Click **Remove**.

Note: You must restart the computer before you reinstall the client.

Appendix A

Windows Installer (.msi) command-line reference

This chapter includes the following topics:

Installing Symantec AntiVirus using command-line parameters

The Symantec AntiVirus client installation programs utilize Windows Installer (.msi) packages for installation and deployment. If you are using the command line to install or deploy an installation package, you can use the standard Windows Installer switches and Symantec-specific parameters to customize the installation.

For the most up-to-date list of Symantec installation commands and parameters, see the Symantec Knowledge Base.

For more information on using the standard Windows Installer commands, see the documentation provided by Microsoft.

Default Symantec AntiVirus client installation

The default Symantec AntiVirus client installation package includes the following installation components:

- Symantec AntiVirus client base files (including the user interface) are installed.
- Symantec AntiVirus Help files are installed.
- Auto-Protect Email Snap-Ins (including Microsoft Exchange, Lotus Notes, and Internet Email) are installed and enabled if the corresponding Microsoft Exchange, Outlook, or Lotus Notes clients are detected. The Internet Email Snap-In is installed by default.
- Symantec Quarantine client files are installed.
- LiveUpdate is installed and updated virus definitions files are downloaded from the Symantec Web site (if the client is connected to the Internet).

The default Symantec AntiVirus client installation package includes the following installation settings:

- The client is installed as an unmanaged client.
- Computer restart is required.
- Auto-Protect is enabled after the computer is restarted.

Default Symantec AntiVirus server installation

The default Symantec AntiVirus server installation package includes the following installation components:

- Symantec AntiVirus server base files (including the user interface) are installed.
- Symantec AntiVirus Help files are installed.
- LiveUpdate is installed and updated virus definitions files are downloaded from the Symantec Web site (if the server is connected to the Internet).

The default Symantec AntiVirus server installation package includes the following installation settings:

- Computer restart is required.
- Auto-Protect is enabled after the computer is restarted.

Windows Installer commands

The Symantec AntiVirus installation packages use the standard Windows Installer commands as well as a set of extensions for command-line installation and deployment.

Windows Installer commands and properties

Table A-1 describes the basic set of commands and properties that are used for Symantec AntiVirus client and server installations. See the Windows Installer documentation for further information on the usage of standard Windows Installer commands and properties.

Table A-1 Commands and properties

Command or property	Description
Msiexec	Windows Installer executable.
Symantec AntiVirus.msi	Symantec AntiVirus installation file.
/i	Install the specified components.
/x	Uninstall the specified components.
/qn	Install silently.
/qb	Include the installation user interface.
/l*v <log filename>	Create a verbose log file, where <log filename> is the name of the log file you want to create.
INSTALLDIR=<path>	Designate a custom path on the target computer where <path> is the specified target directory. If the path includes spaces, use quotation marks.
REBOOT=<value>	Suppress a computer restart after installation, where <value> is a valid argument. The valid arguments include the following: ■ Force: Requires that the computer is restarted. ■ Suppress: Prevents most restarts. ■ ReallySuppress: Prevents all restarts as part of the installation process.

Table A-1 Commands and properties

Command or property	Description
ADDLOCAL= <feature>	Select custom features to be installed, where <feature> is a specified component or list of components. If this property is not used, all applicable features are installed by default. **Note:** When specifying a new feature to be installed, you must include the names of the features that are already installed on the target computer that you want to keep. If you do not specify the features that you want to keep, Windows Installer will remove them. Specifying existing features will not overwrite the installed features. To uninstall an existing feature, use the REMOVE command.
REMOVE=<feature>	Uninstall the previously installed program or a specific feature from the installed program, where <feature> is one of the following: ■ <feature>: Uninstalls the feature or list of features from the target computer. ■ ALL: Uninstalls the program and all of the installed features. This is the default.

Symantec AntiVirus properties

There are many Symantec AntiVirus properties that are used to customize Windows Installer installation packages.

Symantec AntiVirus server properties

Table A-2 describes the properties that are configurable for the Symantec AntiVirus server installation.

Table A-2 Symantec AntiVirus server properties list

Property	Description
INSTALLSERVER=1	Specifies that the installation to be used is the server installation. A value of 0 indicates a client installation.
ENABLEAUTOPROTECT=<val>	Determines whether Auto-Protect is enabled after the installation is complete, where <val> is one of the following values: ■ 1: This enables Auto-Protect after installation. ■ <n>: Any other integer value disables Auto-Protect after installation. The default setting is 1 (enabled).
RUNLIVEUPDATE=<val>	Determines whether LiveUpdate is enabled as part of the installation, where <val> is one of the following: ■ 1: This enables LiveUpdate after installation (default). ■ <n>: Any other integer value disables LiveUpdate after installation. To use this property, Administrator or Power User privileges are required. If you attempt the installation without the correct privileges, the installation may fail without notice. **Note:** LiveUpdate is a required component of the Symantec AntiVirus installation.
NETWORKTYPE=<val>	Describes the management state of the target computer when installation is complete, where <val> is one of the following: ■ 1: Managed ■ 2: Unmanaged (default) ■ 4: Server
SERVERGROUPNAME= <server group name>	Specifies the name of the server group that the target server will join. You can create a new server group by using a unique server name.

Table A-2 Symantec AntiVirus server properties list

Property	Description
SERVERGROUPPASS=<password>	Specifies the password of the server group that the target server will join.
INSTALLDIR=<target directory>	Specifies the installation directory on the target computer. The default directory is C:\Program Files\Symantec AntiVirus. If the path specified contains long file names, use quotation marks around it.

Symantec AntiVirus client properties

Table A-3 describes the properties that are configurable for the Symantec AntiVirus client installation.

Table A-3 Symantec AntiVirus client properties

Property	Description
ENABLEAUTOPROTECT=<val>	Determines whether Auto-Protect is enabled after the installation is complete, where <val> is one of the following values: ■ 1: This enables Auto-Protect after installation. ■ <n>: Any other integer value disables Auto-Protect after installation. The default setting is 1 (enabled).
RUNLIVEUPDATE=<val>	Determines whether LiveUpdate is enabled as part of the installation, where <val> is one of the following: ■ 1: This enables LiveUpdate after installation (default). ■ <n>: Any other integer value disables LiveUpdate after installation. To use this property, Administrator or Power User privileges are required. If you attempt the installation without the correct privileges, the installation may fail without notice. **Note:** LiveUpdate is a required component of the Symantec AntiVirus installation.

Table A-3 Symantec AntiVirus client properties

Property	Description
NETWORKTYPE=<val>	Describes the management state of the target computer when installation is complete, where <val> is one of the following: ■ 1: Managed ■ 2: Unmanaged ■ 4: Server
SERVERNAME=<server group name>	Specifies the name of the pre-existing server group that manages the target computer.
INSTALLDIR=<target directory>	Specifies the installation directory on the target computer. The default directory is C:\Program Files\Symantec AntiVirus. If the path specified contains long file names, use quotation marks around it.

Symantec AntiVirus features

There are many Symantec AntiVirus features that can be installed using a customized Windows Installer package. These features are used by the Windows Installer ADDLOCAL property to specify the features that are installed.

See "Command-line examples" on page 169.

Symantec AntiVirus server features

Table A-4 describes the features that are configurable for the Symantec AntiVirus server installation.

Table A-4 Symantec AntiVirus server features

Feature	Description
SAVMain	Specifies the basic Symantec AntiVirus server files. This feature is required.
SAVUI	Makes the user interface available to the target computer. This feature is optional.
SAVHelp	Include Symantec AntiVirus Help files. This feature is optional.

Symantec AntiVirus client features

Table A-5 describes the features that are configurable for the Symantec AntiVirus client installation.

Table A-5 Symantec AntiVirus client features

Feature	Description
SAVMain	Specifies the basic Symantec AntiVirus client files. This feature is required.
SAVUI	Makes the user interface available to the target computer. This feature is optional.
SAVHelp	Include Symantec AntiVirus Help files. This feature is optional.
EMailTools	Include all of the Auto-Protect Email components. This feature is optional.
OutlookSnapin	Include the Microsoft Exchange Auto-Protect email component. This feature is optional.
NotesSnapin	Include the Lotus Notes Auto-Protect email component. This feature is optional.
Pop3Smtp	Include the Internet Email Auto-Protect component. This feature is optional.
QClient	Include the Symantec Quarantine client. This feature is optional.

Using the log file to check for errors

The Windows Installer creates a log file that can be used to verify whether or not an installation was successful, list the components that were successfully installed, and provide a variety of further details related to the installation package. The log file can be used as an effective tool to troubleshoot an installation package that fails.

If the installation is successful, the log file includes a success entry near the end. If the installation is not successful, an entry is created that indicates that the installation failed.

The log file (sav_inst.log) that is created by the default installation package is added to the \temp directory associated with the user that is running (or deploying) the installation package.

Note: Each time the installation package is executed, the log file is overwritten. Appending an existing log file is not supported.

Identifying the point of failure of an installation

You can use the log file to help identify the component or action that caused an installation to fail.

To identify the point of failure of an installation

1. In a text editor, open the log file that was generated by the installation.
2. Search for the following:

   ```
   VALUE= 3
   ```

   The action that occurred before the line that contains this entry is most likely the action that caused the failure. The lines that appear after this entry are installation components that have been rolled back because the installation was unsuccessful.

Command-line examples

Table A-6 includes commonly used command-line examples.

Table A-6 Command-line examples

Task	Command line
Silently install an unmanaged Symantec AntiVirus client with default settings to c:\SFN.	msiexec/i "Symantec AntiVirus.msi" INSTALLDIR=C:\SFN /qn
Silently install an unmanaged Symantec AntiVirus client that is managed by the SR1 server (having the password hello) with all of the default features except QClient. Do not restart the computer after installation, and do not enable Auto-Protect when the computer is (ultimately) restarted.	msiexec/i "Symantec AntiVirus.msi" ADDLOCAL=SAVMain,SAVUI,SAVHelp, EMailTools,OutlookSnapin,NotesSnapin, Pop3Smtp NETWORKTYPE=2 SERVERNAME= SR1 ENABLEAUTOPROTECT=0 RUNLIVEUPDATE=1 REBOOT=ReallySuppress /qn

Table A-6 Command-line examples

Task	Command line
Silently install a managed Symantec AntiVirus client to the default path that is managed by the SR1 server (having the password hello) with no SAV Help and no Lotus Notes Snap-in. Do not run LiveUpdate, and do not restart the computer automatically.	msiexec/i "Symantec AntiVirus.msi" ADDLOCAL=SAVMain,SAVUI,SAVHelp, EMailTools,OutlookSnapin,Pop3Smtp,QClient NETWORKTYPE=1 SERVERNAME= SR1 ENABLEAUTOPROTECT=1 RUNLIVEUPDATE=0 REBOOT=ReallySuppress /qn

Index